Inland Revenue
Te Tari Taake

17 June 2019

s9(2)(a)

Dear s9(2)(a)

Thank you for your request made under the Official Information Act 1982 (the OIA), received on 29 May 2019. You requested the following:

How many times has your agency/ department been hacked?

The security of the information we hold is paramount and we take great care to protect the integrity of the tax system by guarding the information we hold.

We have interpreted your question to be: "How many times have you detected unauthorised access to your network or systems that would constitute a cyber security incident?". The NZISM[1] defines a cyber security incident as:

> *an occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it or by any other process or system and processes.*

Inland Revenue has not detected any hacking attempts which resulted in the loss of customer data or a breach of Inland Revenue systems.

There continues to be numerous examples of "spam" and "phishing" attempts trying to get customers' details. These are approaches to customers rather than Inland Revenue and have occurred via electronic means, door knocking or phone contact.

Inland Revenue warns taxpayers about the safety and security of their information to prevent against such attempts and does what it can to mitigate them.

How many times has an attempt at a hack been detected at your agency/ department?

Like most other internet-facing organisations, multiple attempted hacks are detected and blocked daily.

[1] The New Zealand Information Security Manual (NZISM) is the New Zealand Government's manual on information assurance and information systems security. www.gcsb.govt.nz/publications/the-nz-information-security-manual/

What are you doing to secure your systems to make sure you're secure?

Inland Revenue has an information security strategy, team, processes, and systems to protect important customer information.

We actively use a wide range of commercial security tools, products and services to ensure the cyber security of our systems.

In addition to the existing security capability that IR has in place, additional investment in Information Security is underway and planned to further reduce risk and respond to cybersecurity threats.

Have you received any instructions to increase your security?

We have not received any instructions to increase our security this year.

Thank you for your request. I trust that the information provided is of assistance to you.

Yours sincerely

Gary Baird
Chief Technology Officer

Inland Revenue
Te Tari Taake

18 July 2019

s9(2)(a)

Dear s9(2)(a)

Thank you for your request made under the Official Information Act 1982 (the OIA), received on 20 June 2019. You requested the following:

> *... all communications, reports, memos, meeting minutes and other documents relating to the 2018 cryptolocker malware attack referred to in this article:*
>
> *https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/*

Summary of events

On Wednesday 9 November 2016, an Inland Revenue staff member, using a Virtual Desktop Infrastructure (VDI) device, clicked on a link in a phishing email resulting in a cryptolocker malware ('Locky') executing. This encrypted 3,734 files on Inland Revenue's X: drive directory, which is a shared network file directory stored on Inland Revenue's South Network Attached Storage (NAS) device.

The issue was identified on Friday 11 November 2016 at approximately 17:00 by an Inland Revenue staff member who noticed that a number of files had the extension of 'THOR'.

Inland Revenue's desktop services provider (DXC) were contacted to ensure that all back-ups were available should a restore be required. Back-ups are kept online for approximately 8 weeks before being archived to tape.

Subsequent investigation by DXC showed that the files had been encrypted on Wednesday 9 November between 12:15 and 12:35.

The staff member who clicked on the email was contacted and they advised that from memory they clicked on a yahoo email on Wednesday 9 November 2016 that could have been the source of the issue.

Two files identified as Locky were removed from the staff member's profile at approximately 14:40 on Friday 11 November 2016.

The staff member's VDI was isolated from the network and a new VDI issued. A virus scan was initiated by DXC; the antivirus console was updated with the latest virus signatures.

A file scan was initiated across both of Inland Revenue's North and South NAS devices and no further Locky encrypted files were found. A Windows search was also undertaken looking for any .THOR extensions.

On Saturday 12 November 2016, DXC removed all encrypted files and the files were restored from backup.

Further information

The files encrypted were on the X: drive (shared file directory) located on the South NAS device and accessed via the staff member's VDI session. No customer information was accessed or could be accessed as a result of this malware issue.

No Inland Revenue applications or systems were breached as a result of this malware issue and no information (customer or Inland Revenue related) was lost.

Since this issue, Inland Revenue has established an awareness programme to educate staff about cyber security. These activities include:

- Security awareness presentations at Inland Revenue sites.
- Instructional videos hosted on Inland Revenue's intranet.
- A series of simulated phishing exercises for randomly selected staff members.
- Regular blogs, updates, and articles about information security hosted on internal communications channels.

Since this issue, Inland Revenue has also decommissioned the older Windows 7 desktop fleet and replaced it with the latest version of Windows 10 and Windows Defender (which are updated automatically), greatly reducing the likelihood of Inland Revenue being infected with a similar malware in the future.

Information being released

I have set out the documents being released in Appendix One. Where information in the documents is withheld, the relevant withholding ground of the OIA is specified in the document. An explanation of the relevant withholding grounds are as follows:

- Section 9(2)(a) – to protect the privacy of natural persons, including deceased persons.

- Section 18(c)(i) – making the requested information available would be contrary to the provisions of a specified enactment, namely Inland Revenue's confidentiality obligation in section 18 of the Tax Administration Act 1994 (TAA). Disclosure of this information does not fall within any of the exceptions to the confidentiality obligation listed in sections 18D to 18J of the TAA.

No public interest in releasing the withheld information has been identified that would be sufficient to outweigh the reasons for withholding.

The slideshow Cyber Security Awareness (item 1) contains some information that is outside the scope of your request. This information has not been considered for release and has not been provided. Additionally, information related to Finance and Expenditure Annual Review questions which are not relevant to your request have also been removed as being outside scope.

Publicly available information

The responses to the Finance and Expenditure Annual Review questions can be found on the Parliament website:

https://www.parliament.nz/resource/en-NZ/52SCFE_EVI_75224_642/41fe9cce4318a5f1042fe8d80309bd4e3ec6f1f8

Accordingly, this information has been withheld under section 18(d) of the OIA, as the information is publicly available.

Right of Review

If you disagree with my decisions on your OIA request, you can ask an Inland Revenue review officer to review my decisions. To ask for an internal review, please email the Commissioner of Inland Revenue at: CommissionersCorrespondence@ird.govt.nz.

Alternatively, under section 28(3) of the OIA, you have the right to ask the Ombudsman to investigate and review my decision. You can contact the office of the Ombudsman by email at: info@ombudsman.parliament.nz.

Thank you for your request. I trust that the information provided is of assistance to you.

Yours sincerely

Gary Baird
Chief Technology Officer

Appendix One – Information being released

Item	Date	Document type	Document title / email subject
1.	July 2017	Slideshow	*Cyber Security Awareness*
2.	21 Dec 2017	Email chain	*FEC Questions – IT&C Responses for Review & Approval*
3.	21 Dec 2017	Email chain	*FEC Standard Annual Review Questions*
4.	26 Feb 2018	Email	*2017 Annual Review Standard Question Allocation – IT&C responses FINAL*
5.	26 Feb 2018	Email chain	*Cryptolocker hits IR*
6.	26 Feb 2018	Email	*IRD Security in the press*
7.	26 Feb 2018	Email chain	*media query*
8.	26 Feb 2018	Email chain	*In case you hadn't seen this*
9.	26 Feb 2018	Email chain	*media query*
10.	27 Feb 2018	Email chain	*media query*
11.	27 Feb 2018	Email chain	*media query*
12.	27 Feb 2018	Email chain	*media query*
13.	9 Apr 2018	Email chain	*media query*

Cyber Security Awareness

Doug Hammond
Chief Information Security Officer (CISO)
July 2017

Cyber Attacks

They happen, and we're vulnerable

SECURE iT

We've been hit already....

November Phishing attack - the Details

1. In November last year one of our people opened **personal email** and clicked on phishing link.
2. Ransomware was installed.
3. X: drive was encrypted – 3,500 files s 18(c)(i) s 18(c)(i)
4. Ransomware software s 18(c)(i) s 18(c)(i) deleted by the Anti-virus.
5. Files were reinstalled through backups within one hour.

SECURE iT

Outside scope

From: Doug Hammond
Sent: Thursday, 21 December 2017 8:41 AM
To: Yogesh Anand; s 9(2)(a)
Subject: RE: FEC Questions - IT&C Responses for Review & Approval

Hi

Yes, happy with these edits – good to go s 9(2)(a)

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)
55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: Yogesh Anand
Sent: Thursday, 21 December 2017 7:36 a.m.
To: Doug Hammond; s 9(2)(a)
Subject: RE: FEC Questions - IT&C Responses for Review & Approval

Thanks – this looks fine. Outside scope . Please review and let me know if this is not correct.
cheers

Best regards
Yogesh

Director Solutions | Information Technology & Change
s 9(2)(a)

From: Doug Hammond
Sent: Wednesday, 20 December 2017 3:59 p.m.
To: Yogesh Anand; s 9(2)(a)
Subject: RE: FEC Questions - IT&C Responses for Review & Approval

Hi

Next revision attached. Let me know if this works

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: Yogesh Anand
Sent: Wednesday, 20 December 2017 3:38 p.m.
To: Doug Hammond; s 9(2)(a)
Subject: RE: FEC Questions - IT&C Responses for Review & Approval

Thanks Doug, a couple of comments.

Outside scope

- Finally, re the cryptolocker issue – what was the control put in place to top it happening again otherwise it sound like we just recovered the files and then did nothing.

cheers

Best regards
Yogesh

Director Solutions | Information Technology & Change
s 9(2)(a)

From: Doug Hammond
Sent: Wednesday, 20 December 2017 3:28 p.m.
To: s 9(2)(a); s 9(2)(a); Yogesh Anand
Subject: RE: FEC Questions - IT&C Responses for Review & Approval

Hi

Edits and comments attached.

Yogesh – have a look at the changes and comments I have made. Outside scope

Outside scope

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)
55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: s 9(2)(a)
Sent: Wednesday, 20 December 2017 1:14 p.m.
To: Doug Hammond; s 9(2)(a)
Subject: FW: FEC Questions - IT&C Responses for Review & Approval
Importance: High

Hi both

Can you please have a look at the comments from Yogesh on questions 23, page one and 28, page four?

Thanks
s 9(2)(a)

| Performance & Capability Team Manager| Information Technology & Change
s 9(2)(a)

From: Yogesh Anand
Sent: Wednesday, 20 December 2017 12:47 p.m.
To: s 9(2)(a)
Cc: Don Burns
Subject: RE: FEC Questions - IT&C Responses for Review & Approval

Thanks s 9(2)(a) – some comments included.
cheers

Best regards
Yogesh

Director Solutions | Information Technology & Change
s 9(2)(a)

From: s 9(2)(a)
Sent: Wednesday, 20 December 2017 10:22 a.m.
To: Yogesh Anand
Cc: Don Burns
Subject: FEC Questions - IT&C Responses for Review & Approval

Hi Yogesh

Hope your well, not long to go now!

I have attached our IT&C FEC responses for your review and approval which are due back to GES by COB 17 January 2018.

It would be great if you could please review these either before you go on leave this week or your first week back in the office.

Wishing you a happy Christmas and a relaxing break.

Thanks
s 9(2)(a)

Outside scope

From: Don Burns
Sent: Thursday, 21 December 2017 11:39 AM
To: s 9(2)(a) ; Doug Hammond
Subject: FW: FEC Standard Annual Review Questions
Attachments: 2017 Annual Review Standard Question Allocation - ITC responses FINAL.docx

Hi,

Please see the attached – thanks for your assistance in providing the data.

Regards

Don

From: s 9(2)(a)
Sent: Thursday, 21 December 2017 10:41 a.m.
To: Ministerial Services
Cc: Don Burns
Subject: RE: FEC Standard Annual Review Questions

Hi there

Please see the attached response from IT&C. If you have any queries, I'll be back in the office from the 4th and will be able to assist.

Have a happy Christmas and relaxing break.

Thanks
s 9(2)(a)
| Performance & Capability Team Manager| Information Technology & Change
s 9(2)(a)

From: Ministerial Services
Sent: Friday, 15 December 2017 10:21 a.m.
To: s 9(2)(a) ; Gary Baird; Greg James; Cath Atkins; Martin Smith; Mary Craig; Mike Cunnington; Lara Ariell; Mark Daldorf; Alan Pinder; Andrew Stott; s 9(2)(a) ; Marilyn Jones; s 9(2)(a) ; Don Burns; Nigel Mehta-Wilson; Don Burns; s 9(2)(a) ; Samantha van Riet; s 9(2)(a) ; Charlene Harvey; s 9(2)(a) s 9(2)(a)
Cc: s 9(2)(a)
Subject: FEC Standard Annual Review Questions

Good morning everyone,

We have received notification from the Clerk of the Finance and Expenditure Committee (FEC) about the annual review of Inland Revenue's operation and performance for the 2016/17 year.

A hearing of evidence has been confirmed on Thursday 8 February 2018.

We have also been provided with the standard annual review questions for the hearing. As usual the timeframe for responding to these questions is very short. I have allocated the questions to the Tier 2 managers for the relevant business groups (attached).

We have also highlighted in yellow questions that are slightly different this year to previous years. Hopefully this will assist staff preparing responses. Most of the differences relate to the data requested for back years – **whereas last year the FEC asked for data going back three years, this time they have asked for data going back four years in many instances.**

If any of the questions are incorrectly allocated, please contact myself or Kerryn McIntosh-Watt as soon as possible so that we can reallocate the questions and update our records.

A response template is attached. We would appreciate if all draft responses to these questions **and hot topics that have not already been provided to GES, ore require updating,** can be provided to us by close of business on **Wednesday 17 January**. I realise this timeframe is short, however it is dictated to us by the FEC. If you think you will have difficulty meeting this timeframe, please contact myself or Kerryn as soon as possible.

GES is at its Xmas party for the rest of today. We will send out a list of questions individualised to Business Units on Monday morning.

If you have any questions or concerns, please contact myself or Kerryn McIntosh-Watt to discuss.

Thanks and kind regards,

s 9(2)(a) **|Senior Ministerial Advisor | Government & Executive Services**
Stakeholder Relations | Corporate Integrity and Assurance | Inland Revenue
Level 10, Asteron Centre | 55 Featherston Street | Wellington
s 9(2)(a)

Outside scope

From: Don Burns
Sent: Monday, 26 February 2018 12:03 PM
To: Doug Hammond
Subject: 2017 Annual Review Standard Question Allocation - IT&C responses FINAL
Attachments: 2017 Annual Review Standard Question Allocation - IT&C responses FINAL.docx

Hi Doug,

See attached.

The response does make reference to November 2017.

Regards

Don

Outside scope

From: Doug Hammond
Sent: Monday, 26 February 2018 10:43 AM
To: Alan Pinder
Subject: RE: Cryptolocker hits IR

Hi

Yes we did lots of comms on this. Note that the article is wrong – the breach occurred in November 2016. I personally briefed Mary at the time. I guess the reason it doesn't come to memory is that the breach was 16 months ago, not 4 months ago.

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: Alan Pinder
Sent: Monday, 26 February 2018 10:05 a.m.
To: Doug Hammond
Subject: Cryptolocker hits IR

Hi Doug,

Mary and I noticed this story in the clippings this morning:

https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

Neither of us could remember getting notification at the time that this had happened. Now it's always possible we did, and just don't recall now. What's your recollection of the information flow on this?

Cheers

Alan

Alan Pinder | Chief Advisor to Deputy Commissioner Corporate Integrity and Assurance | Inland Revenue
s 9(2)(a)

s 9(2)(a), Outside

From: Doug Hammond
Sent: Monday, 26 February 2018 12:15 PM
To: Information Security - All Staff
Subject: IRD Security in the press [UNCLASSIFIED]

https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

Outside scope

From: s 9(2)(a)
Sent: Monday, 26 February 2018 12:33 PM
To: Doug Hammond
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Sorry it was Locky. Encrypted files had the extension of .THOR

CHeers

s 9(2)(a)
Account Security Officer
Governance and Customer Compliance, ANZ
DXC Security

T s 9(2)(a)

DXC Technology
Auckland, New Zealand

dxc.technology / Twitter / Facebook / LinkedIn

From: s 9(2)(a)
Sent: Monday, 26 February 2018 12:29 PM
To: 'Doug Hammond' s 9(2)(a)
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Hi Doug,

Just looking for the timeline of events. The Malware was THOR. It was a new variant at the time and was not picked up by SEP straight away. IT was picked up by SEP about 2 days later when they released a new signature.

I will get the facts for you

Cheers,

s 9(2)(a)
Account Security Officer
Governance and Customer Compliance, ANZ
DXC Security

T s 9(2)(a)

DXC Technology
Auckland, New Zealand

dxc.technology / Twitter / Facebook / LinkedIn

From: Doug Hammond s 9(2)(a)
Sent: Monday, 26 February 2018 12:13 PM
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: FW: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Hi s 9(2)(a)

I need some technical details on the Cryptolocker breach we had in November 2016. See emails below. Can you provide these?

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: Don Burns
Sent: Monday, 26 February 2018 11:54 a.m.
To: Doug Hammond
Subject: FW: media query

Doug,

Please see email below and the query from Rob O'Neill.

Can you consider and respond to s 9(2)(a)

Regards

Don

From: s 9(2)(a)
Sent: Monday, 26 February 2018 10:08 a.m.
To: Don Burns
Subject: media query

Hi Don,

We've had a query this morning from Rob O'Neill of Reseller News about Q28 in the FEC annual review hearing written questions, and s 9(2)(a) tells me you co-ordinated the response.

He's wanting to know exactly what type of cryptolocker was involved in the malware incident referred to in the answer.

He's already covered it in this story - https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

Are you able to point me in the right direction of who would be able to provide the information? And perhaps there may need to be some discussion at your end as to whether this information is released.

Certainly if we do answer it, we could provide some additional information about the staff education efforts we undertake to try to prevent such security breaches. He has already referenced in the article above that our performance has improved in this regard over the past five years.

Cheers, s 9(2)(a)

s 9(2)(a) | Senior Media Advisor, Marketing & Communications | Inland Revenue
s 9(2)(a)

Inland Revenue
Te Tari Taake

Outside scope

From: s 9(2)(a)
Sent: Monday, 26 February 2018 1:36 PM
To: Doug Hammond; s 9(2)(a)
Subject: In case you hadn't seen this

https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

s 9(2)(a)
Partner | National Leader - Cyber, Privacy and Resilience
Deloitte
s 9(2)(a)

Sent from my iPhone

Outside scope

From: s 9(2)(a)
Sent: Monday, 26 February 2018 4:40 PM
To: Doug Hammond
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

I will get our change manager to extract the timeline form the actual incident from when it was raised.

Regards,

s 9(2)(a)
Account Security Officer
Governance and Customer Compliance, ANZ
DXC Security

T s 9(2)(a)

DXC Technology
Auckland, New Zealand

dxc.technology / Twitter / Facebook / LinkedIn

From: Doug Hammond s 9(2)(a)
Sent: Monday, 26 February 2018 4:24 PM
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

The timeline would be useful. I assume it exists and can just be sent to me?

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: s 9(2)(a)
Sent: Monday, 26 February 2018 3:45 p.m.
To: Doug Hammond
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Hi Doug,

Do you want the timeline of events occurring or just the facts on what happened, was done to rectify etc.

Cheers

s 9(2)(a)
Account Security Officer
Governance and Customer Compliance, ANZ
DXC Security

T s 9(2)(a)

DXC Technology
Auckland, New Zealand

dxc.technology / Twitter / Facebook / LinkedIn

From: Doug Hammond s 9(2)(a)
Sent: Monday, 26 February 2018 12:13 PM
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: FW: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Hi s 9(2)(a)

I need some technical details on the Cryptolocker breach we had in November 2016. See emails below. Can you provide these?

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

From: Don Burns
Sent: Monday, 26 February 2018 11:54 a.m.
To: Doug Hammond
Subject: FW: media query

Doug,

Please see email below and the query from Rob O'Neill.

Can you consider and respond to s 9(2)(a)

Regards

Don

From: s 9(2)(a)
Sent: Monday, 26 February 2018 10:08 a.m.
To: Don Burns
Subject: media query

Hi Don,

We've had a query this morning from Rob O'Neill of Reseller News about Q28 in the FEC annual review hearing written questions, and s 9(2)(a) tells me you co-ordinated the response.

He's wanting to know exactly what type of cryptolocker was involved in the malware incident referred to in the answer.

He's already covered it in this story - https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

Are you able to point me in the right direction of who would be able to provide the information? And perhaps there may need to be some discussion at your end as to whether this information is released.

Certainly if we do answer it, we could provide some additional information about the staff education efforts we undertake to try to prevent such security breaches. He has already referenced in the article above that our performance has improved in this regard over the past five years.

Cheers, s 9(2)(a)

s 9(2)(a) | Senior Media Advisor, Marketing & Communications | Inland Revenue
s 9(2)(a)

Inland Revenue
Te Tari Taake

This email and any attachment may contain confidential information. If you have received this email or any attachment in error, please delete the email / attachment, and notify the sender. Please do not copy, disclose or use the email, any attachment, or any information contained in them. Consider the environment before deciding to print: avoid printing if you can, or consider printing double-sided. Visit us online at ird.govt.nz

Outside scope

From: s 9(2)(a)
Sent: Tuesday, 27 February 2018 5:51 AM
To: Doug Hammond
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Doug,

I have gone through my e-mails. There is no record of the loki incident since I have been on board in my e-mails.

My first awareness of this was the December security meeting with HP s 9(2)(a) and I were in attendance.

Having said this, I can touch base with the MIM team for any information they may have.

Cheers,
s 9(2)(a)

From: Doug Hammond
Sent: Monday, 26 February 2018 4:24 p.m.
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

The timeline would be useful. I assume it exists and can just be sent to me?

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: s 9(2)(a)
Sent: Monday, 26 February 2018 3:45 p.m.
To: Doug Hammond
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Hi Doug,

Do you want the timeline of events occurring or just the facts on what happened, was done to rectify etc.

Cheers

s 9(2)(a)
Account Security Officer
Governance and Customer Compliance, ANZ

DXC Security

T s 9(2)(a)

DXC Technology
Auckland, New Zealand

dxc.technology / Twitter / Facebook / LinkedIn

From: Doug Hammond s 9(2)(a)
Sent: Monday, 26 February 2018 12:13 PM
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: FW: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Hi s 9(2)(a)

I need some technical details on the Cryptolocker breach we had in November 2016. See emails below. Can you provide these?

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: Don Burns
Sent: Monday, 26 February 2018 11:54 a.m.
To: Doug Hammond
Subject: FW: media query

Doug,

Please see email below and the query from Rob O'Neill.

Can you consider and respond to s 9(2)(a)

Regards

Don

From: s 9(2)(a)
Sent: Monday, 26 February 2018 10:08 a.m.
To: Don Burns
Subject: media query

Hi Don,

We've had a query this morning from Rob O'Neill of Reseller News about Q28 in the FEC annual review hearing written questions, and s 9(2)(a) tells me you co-ordinated the response.

He's wanting to know exactly what type of cryptolocker was involved in the malware incident referred to in the answer.

He's already covered it in this story - https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

Are you able to point me in the right direction of who would be able to provide the information? And perhaps there may need to be some discussion at your end as to whether this information is released.

Certainly if we do answer it, we could provide some additional information about the staff education efforts we undertake to try to prevent such security breaches. He has already referenced in the article above that our performance has improved in this regard over the past five years.

Cheers, s 9(2)(a)

s 9(2)(a) | Senior Media Advisor, Marketing & Communications | Inland Revenue
s 9(2)(a)

Inland Revenue
Te Tari Taake

Outside scope

From: s 9(2)(a)
Sent: Tuesday, 27 February 2018 10:07 AM
To: Doug Hammond
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Here is the timeline from the incident report

Incident Report

Incident Overview (Of the Incident and restoration activities)	5:10PM – IR ICT members 9(2)(a) emailed Security team regarding .thor files found in the location of X:\ITAM Temp File Location\Media. 5:18PM – HPE Security contacted Service Desk to raise a P2 incident and informed the account team. HPE account team advised IR Incident Management team accordingly. 5:59PM – P2 incident AU-IM009155942 raised. Investigation showed the Ransomware files were encrypted files related to the Locky ransomware. Any files with .THOR had already been encrypted. Antivirus console investigated: it was identified that 2 copies of Locky had been cleared from the VDI profile of s 9(2)(a) in the afternoon of 11/11. HPE isolated s 9(2)(a)'s VDI from the network and performed a virus scan HPE further completed the following - 1. Ensured that Antivirus console has been updated with the latest virus signatures 2. Started a virus scan for shares in both north and south NAS, as well as all Exchange mailboxes 3. Started a windows search of anything with .THOR extension. Files with a .THOR extension were quickly discovered in the PACKAGES and ITAM Temp Files folders on the STH NAS. The final total was 3734 encrypted files. The majority of these had s 9(2)(a) s 9(2)(a) as the file owner. HPE isolated s 9(2)(a)'s VDI from the network and performed a virus scan performed across it; no further infection was found.
Customer Impact (How did the Incident(s) affect the Customer's business?)	3734 files in the ITAM Temp Files and the Packages folders were encrypted. These were removed and restored form back up.

Service Recovery Actions

Date/Time	Action	Outcome	Capability Team(s)
11/11 17:15	Investigate files with a .THOR extension	.THOR files found to be encrypted files related to the Locky ransomware	Security
11/11 18:00	Investigate antivirus SEPM console	it was identified that 2 copies of Locky had been cleared from the VDI profile of s 9(2)(a) in the afternoon of 11/11	Security
11/11 18:30	Isolate s 9(2)(a)'s VDI from the network and performed a virus scan	No further infection was found	Security
11/11 19:00	Ensure that antivirus console has been updated with the latest virus signatures	Virus signatures updated	Security

11/11 20:30	Start a virus scan for shares in both north and south NAS, as well as all Exchange mailbox	Virus scan run, 3734 encrypted files found in the PACKAGES and ITAM Temp Files folders on the south NAS	Security
11/11 21:00	Start a windows search of anything with .THOR extension	Virus scan run, 3734 encrypted files found in the PACKAGES and ITAM Temp Files folders on the south NAS	Security
12/11 13:00	Remove the encrypted files found	Encrypted files removed	Wintel
12/11 17:00	Recover the folders containing encrypted files from backups to a separate location	Relevant folders recovered from backup to a separate location	Back & Recovery

And here is the commentary on the incident and investigations.

s 9(2)(a) called me just after 17:00 on Friday 11/11/2016 explaining she was looking in the ITAMS folders and noticed a lot of files with a alpha number name and the extension of THOR. My investigation showed these are files encrypted by the Locky ransomware (quick google search showed articles by Symantec, McAfee and other AV vendors). The Back-up and Restore team were notified to ensure all back-ups were available should a restore be required. Back-ups are kept online for approx. 8 weeks before being passed off to tape.

Investigation of the encrypted files showed that had been encrypted on Wednesday 9th November starting at 12:15 pm and encryption stopped at approx. 12:35 pm. To ensure we had identified all encrypted files DXC started a files search of al container on the NAS looking for any files with the extension of .THOR. A total of 3734 files were identified, mainly in the ITAM Temp folder and the Packages folder on the NAS.
A check of the SEP management console showed 2 files had been identified as Locky and removed from the profile of s 9(2)(a) on Friday 11/11 at approx. 14:30. Discussions with Symantec showed they had released a new signature on Friday 11/11 about 10:00am NZ time. This signature was specifically to identify and remove a new variant of Locky. This is what was found on s 9(2)(a) 's profile s 9(2)(a) 's VDI was isolated form the network and a new VDI was issued to him. IR were to interview s 9(2)(a) to determine where the ransomware came from. From memory s 9(2)(a) advised he did click on a yahoo e-mail that could have been the source on the Wednesday.

File searches of the NAS did not pick up any more encrypted files. A SEP scan was perform across the NAS, numerous malware files were found and removed but there were no more instances of Locky identified. On Saturday afternoon DXC were asked to remove the encrypted files and restore from back-ups. All back-ups were restored by Sunday afternoon.

s 18(c)(i)

If you wish to discuss any of the above please let me know.

Regards,

s 9(2)(a)
Account Security Officer
Governance and Customer Compliance, ANZ
DXC Security

T s 9(2)(a)

DXC Technology
Auckland, New Zealand

dxc.technology / Twitter / Facebook / LinkedIn

From: Doug Hammond s 9(2)(a)
Sent: Monday, 26 February 2018 4:24 PM
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

The timeline would be useful. I assume it exists and can just be sent to me?

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: s 9(2)(a)
Sent: Monday, 26 February 2018 3:45 p.m.
To: Doug Hammond
Cc: s 9(2)(a)
Subject: RE: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Hi Doug,

Do you want the timeline of events occurring or just the facts on what happened, was done to rectify etc.

Cheers

s 9(2)(a)
Account Security Officer
Governance and Customer Compliance, ANZ
DXC Security

T s 9(2)(a)

DXC Technology
Auckland, New Zealand

dxc.technology / Twitter / Facebook / LinkedIn

From: Doug Hammond s 9(2)(a)
Sent: Monday, 26 February 2018 12:13 PM
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: FW: media query [IN CONFIDENCE – RELEASE EXTERNAL]

Hi s 9(2)(a)

I need some technical details on the Cryptolocker breach we had in November 2016. See emails below. Can you provide these?

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)
55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: Don Burns
Sent: Monday, 26 February 2018 11:54 a.m.
To: Doug Hammond
Subject: FW: media query

Doug,

Please see email below and the query from Rob O'Neill.

Can you consider and respond to s 9(2)(a)

Regards

Don

From: s 9(2)(a)
Sent: Monday, 26 February 2018 10:08 a.m.
To: Don Burns
Subject: media query

Hi Don,

We've had a query this morning from Rob O'Neill of Reseller News about Q28 in the FEC annual review hearing written questions, and s 9(2)(a) tells me you co-ordinated the response.

He's wanting to know exactly what type of cryptolocker was involved in the malware incident referred to in the answer.

He's already covered it in this story - https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

Are you able to point me in the right direction of who would be able to provide the information? And perhaps there may need to be some discussion at your end as to whether this information is released.

Certainly if we do answer it, we could provide some additional information about the staff education efforts we undertake to try to prevent such security breaches. He has already referenced in the article above that our performance has improved in this regard over the past five years.

Cheers, s 9(2)(a)

s 9(2)(a) | Senior Media Advisor, Marketing & Communications | Inland Revenue
s 9(2)(a)

Inland Revenue
Te Tari Taake

This email and any attachment may contain confidential information. If you have received this email or any attachment in error, please delete the email / attachment, and notify the sender. Please do not copy, disclose or use the email, any attachment, or any information contained in them. Consider the environment before deciding to print: avoid printing if you can, or consider printing double-sided. Visit us online at ird.govt.nz

Outside scope

From: s 9(2)(a)
Sent: Tuesday, 27 February 2018 1:11 PM
To: Doug Hammond
Subject: RE: media query

Brilliant

From: Doug Hammond
Sent: Tuesday, 27 February 2018 1:10 p.m.
To: s 9(2)(a)
Cc: Don Burns
Subject: RE: media query

Thanks s 9(2)(a) – happy for you to send it directly

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)
55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: s 9(2)(a)
Sent: Tuesday, 27 February 2018 1:08 p.m.
To: Doug Hammond
Cc: Don Burns
Subject: RE: media query

Hi Doug,

Thanks for all this info – I will condense the good stuff we're doing a little as it's probably too much information for his purposes. Are you happy for me to send that directly to the reporter or would you like to see my abbreviated version first?

Cheers, s 9(2)(a)

From: Doug Hammond
Sent: Tuesday, 27 February 2018 1:01 p.m.
To: Don Burns; s 9(2)(a)
Subject: RE: media query

Hi s 9(2)(a)

The cryptolocker variant we were dealing with was called 'Locky'. I've attached the full incident report from DXC for your information.

The good stuff we have done since this infection is summarised as:
Last year a 3 year security awareness programme was established. Since then we have run security awareness presentations across nearly all IR offices and also run after hours Netsafe sessions for IR

staff and families at the bigger sites. We created and released two Terminal-ator videos to all our staff to mark 2017 Cyber Smart week together with articles posted and email communication on each day covering key topics. Since, November 2016 there have been three simulated phishing exercises for a cross section of randomly selected staff across all IR sites and we have plans for more of these tests this year. We ran a range of blogs and articles on information security with key highlights being a digital foot printing exercise performed on our CTO and a blog run by the CISO using his personal experiences.

We have shared our learning with a number of government agencies including, CAA, Land Transport NZ, Ministry of Education, Customs and DIA.

We are developing short presentations on security related key human behavioural risks for people leaders to take their staff through and looking at 4 risks per year. We are also in the process of developing a new induction module which will be used for both as induction and refresher. Desktop and simulation exercises are also underway for major security incidents involving the Crisis Management Team.

Let me know if you need anything else.

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)

55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

Inland Revenue
Te Tari Taake

From: Don Burns
Sent: Monday, 26 February 2018 11:54 a.m.
To: Doug Hammond
Subject: FW: media query

Doug,

Please see email below and the query from Rob O'Neill.

Can you consider and respond to s 9(2)(a)

Regards

Don

From: s 9(2)(a)
Sent: Monday, 26 February 2018 10:08 a.m.
To: Don Burns
Subject: media query

Hi Don,

We've had a query this morning from Rob O'Neill of Reseller News about Q28 in the FEC annual review hearing written questions, and s 9(2)(a) tells me you co-ordinated the response.

He's wanting to know exactly what type of cryptolocker was involved in the malware incident referred to in the answer.

He's already covered it in this story - https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

Are you able to point me in the right direction of who would be able to provide the information? And perhaps there may need to be some discussion at your end as to whether this information is released.

Certainly if we do answer it, we could provide some additional information about the staff education efforts we undertake to try to prevent such security breaches. He has already referenced in the article above that our performance has improved in this regard over the past five years.

Cheers, s 9(2)(a)

s 9(2)(a) | Senior Media Advisor, Marketing & Communications | Inland Revenue
s 9(2)(a)

Inland Revenue
Te Tari Taake

Outside scope

From: s 9(2)(a)
Sent: Monday, 9 April 2018 11:09 AM
To: Don Burns
Subject: RE: media query

Hi Don,

This is what I sent the reporter:

The cryptolocker variant we were dealing with was called Locky. The affected files were isolated, removed and backed up within 24 hours of the ransomware being discovered.
Since this incident we have established a three-year awareness programme to further educate staff about cyber security. The activities undertaken to date include: security awareness presentations at nearly all IR sites; instructional videos hosted on our intranet coinciding with 2017 Cyber Smart Week; a series of simulated phishing exercises for randomly selected staff; and regular blogs, updates and articles about information security hosted on internal communications channels.

Let me know if there's anything else I can do to help.

Cheers, s 9(2)(a)

From: Don Burns
Sent: Monday, 9 April 2018 11:05 a.m.
To: s 9(2)(a)
Subject: RE: media query

Hi s 9(2)(a)

I am just working on an OIA (security related question).

Would you be able to send me the abbreviated version that you sent the report (see below) ?

Thanks – appreciated.

Don

From: Doug Hammond
Sent: Tuesday, 27 February 2018 1:10 p.m.
To: s 9(2)(a)
Cc: Don Burns
Subject: RE: media query

Thanks s 9(2)(a) – happy for you to send it directly

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)
55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

From: s 9(2)(a)
Sent: Tuesday, 27 February 2018 1:08 p.m.
To: Doug Hammond
Cc: Don Burns
Subject: RE: media query

Hi Doug,

Thanks for all this info – I will condense the good stuff we're doing a little as it's probably too much information for his purposes. Are you happy for me to send that directly to the reporter or would you like to see my abbreviated version first?

Cheers, s 9(2)(a)

From: Doug Hammond
Sent: Tuesday, 27 February 2018 1:01 p.m.
To: Don Burns; s 9(2)(a)
Subject: RE: media query

Hi s 9(2)(a)

The cryptolocker variant we were dealing with was called 'Locky'. I've attached the full incident report from DXC for your information.

The good stuff we have done since this infection is summarised as:
Last year a 3 year security awareness programme was established. Since then we have run security awareness presentations across nearly all IR offices and also run after hours Netsafe sessions for IR staff and families at the bigger sites. We created and released two Terminal-ator videos to all our staff to mark 2017 Cyber Smart week together with articles posted and email communication on each day covering key topics. Since, November 2016 there have been three simulated phishing exercises for a cross section of randomly selected staff across all IR sites and we have plans for more of these tests this year. We ran a range of blogs and articles on information security with key highlights being a digital foot printing exercise performed on our CTO and a blog run by the CISO using his personal experiences.

We have shared our learning with a number of government agencies including, CAA, Land Transport NZ, Ministry of Education, Customs and DIA.

We are developing short presentations on security related key human behavioural risks for people leaders to take their staff through and looking at 4 risks per year. We are also in the process of developing a new induction module which will be used for both as induction and refresher. Desktop and simulation exercises are also underway for major security incidents involving the Crisis Management Team.

Let me know if you need anything else.

Hei konā rā

Doug Hammond
Chief Information Security Officer | Information Technology & Change | Inland Revenue
s 9(2)(a)
55 Featherston Street, PO Box 2198, Wellington 6140, New Zealand

From: Don Burns
Sent: Monday, 26 February 2018 11:54 a.m.
To: Doug Hammond
Subject: FW: media query

Doug,

Please see email below and the query from Rob O'Neill.

Can you consider and respond to s 9(2)(a)

Regards

Don

From: s 9(2)(a)
Sent: Monday, 26 February 2018 10:08 a.m.
To: Don Burns
Subject: media query

Hi Don,

We've had a query this morning from Rob O'Neill of Reseller News about Q28 in the FEC annual review hearing written questions, and s 9(2)(a) tells me you co-ordinated the response.

He's wanting to know exactly what type of cryptolocker was involved in the malware incident referred to in the answer.

He's already covered it in this story - https://www.reseller.co.nz/article/633824/cryptolocker-malware-hits-ird-locks-3500-files/

Are you able to point me in the right direction of who would be able to provide the information? And perhaps there may need to be some discussion at your end as to whether this information is released.

Certainly if we do answer it, we could provide some additional information about the staff education efforts we undertake to try to prevent such security breaches. He has already referenced in the article above that our performance has improved in this regard over the past five years.

Cheers, s 9(2)(a)

s 9(2)(a) | Senior Media Advisor, Marketing & Communications | Inland Revenue
s 9(2)(a)

Inland Revenue
Te Tari Taake

2 September 2019

s9(2)(a)

Dear s9(2)(a)

Thank you for your request made under the Official Information Act 1982 (the Act), received on 9 August 2019. You requested the following:

1. *What are the specific and detailed steps taken by IRD to prevent their clients from being "cut-off" during a phone call?*
2. *How has IRD handled the complaint I made about this, this morning via secure mail?*
3. *Will IRD pay me $120 + GST for the 45 minutes of time this wastes, as this is what my time costs for providing accounting services to my clients, and I do not feel comfortable enough passing the cost of having my time wasted by IRD on to my clients. However, I do feel comfortable asking IRD for this money.*

Question One

Inland Revenue's Contact Centre system is designed to ensure a call is not cut off, unless the caller or staff member terminates the call. Inland Revenue has a live 'failover system' between two data centres, where the Contact Centre technology is hosted. This means that if there is a service disruption at one data centre, the calls are live routed to the other data centre.

Customer Service Officers (CSOs) are given robust customer service training which includes treating all callers with empathy and respect. This ensures that staff operate within Inland Revenue's Charter. No specific safe-guards are in place to prevent calls from being terminated as staff do need the ability to end calls. If a caller behaves in an abusive, threatening, or otherwise inappropriate manner, the CSO will advise them that their behaviour is inappropriate. If this behaviour continues then the CSO may terminate the call. If it is identified that a call was ended without any justification, this would be looked into and feedback and coaching would be provided to that CSO.

Question Two

I understand your complaint has been responded to by a CSO in the Complaints Management team.

Question Three

While I acknowledge there has been some delays during our recent period of high demand, Inland Revenue will not make a payment as there are a variety of options to assist tax agents to self-manage, for example:

- The tax agent line call wait times are advertised to help you identify the best time to contact Inland Revenue;
- A list of top solutions and updates on the most common issues tax agents are facing are published on Inland Revenue's website here: https://www.classic.ird.govt.nz/campaigns/2019/top-solutions/

- If wait times are too long, tax agents are offered a call-back service; and
- Secure mail in myIR is available for non-urgent or more technical issues.

If these options are not suitable to your specific situation, your dedicated Inland Revenue Account Manager is available to help.

Thank you for your request. I trust this information is of assistance to you.

Yours sincerely

Bernie Newman
Customer Segment Lead - Individuals

Inland Revenue
Te Tari Taake

7 October 2019

s9(2)(a)

Dear s9(2)(a)

Thank you for your request made under the Official Information Act 1982 (OIA), received on 4 September 2019. You requested the following:

> *Does IRD keep metrics on average wait times for phone calls, abandonment data, response time for letters, etc... I would like a copy of this data for the last 12 months.*

Enclosed is a spreadsheet containing various metrics for phone calls to Inland Revenue calls centres for the 12-month period September 2018 to August 2019 (inclusive) including:

- Attempted calls
- Capped calls (the number of calls by customers calling Inland Revenue call centres which were disconnected before entering the queue)
- Accepted calls
- Abandoned calls (the number of calls abandoned by customers calling Inland Revenue call centres)
- Answered calls
- Average speed to answer
- Average customer time (from first connecting the call, to resolving the issue and both parties disengaging the call)

Also enclosed is a spreadsheet containing the number of electronic and paper correspondence sent in the 12-month period September 2018 to August 2019, broken down by week.

Please note, the data for electronic and paper correspondence was obtained from Inland Revenue's START and FIRST systems. As the data was obtained from two different sources, we are unable to validate whether a specific case was present in both systems. This is due to a potential co-existence solution to complete the task and therefore, the total volumes should not be combined.

Thank you for your request. I trust that the information provided is of assistance to you.

Yours sincerely

James Barker
Group Lead – Capability & Outcomes

Ref: 20OIA1075

Inland Revenue
Te Tari Taake

6 December 2019

s9(2)(a)

Dear s9(2)(a)

Thank you for your request made under the Official Information Act 1982 (the OIA), received on 25 October 2019. You requested the following:

> *any communications or directives the IRD might have issued regarding Uber, Uber drivers or Mitch Cooper since 2018*

On 8 November 2019, you clarified your request to the following:

> *any communications or directives the IRD might have issued regarding Uber, Uber drivers or Mitch Cooper. Specifically, anything related to their tax structuring, the application of GST, or directives around whether to use or not use Uber, between 1 Jan 2015 and 1 November 2019*

Your request for information relating to Uber, Uber drivers, or Mitch Cooper is refused under section 18(c)(i) of the OIA, as releasing this information would be contrary to the provisions specified in section 18 of the Tax Administration Act 1994 (TAA).

Information related to the affairs of a person or entity, that may be regarded as private or commercially sensitive, is considered sensitive revenue information and is confidential under section 18 of the TAA. Disclosure of this information does not fall within any of the exceptions to the confidentiality obligation listed in sections 18D to 18J of the TAA.

Additionally, Inland Revenue has not issued any directives to staff about whether or not to use Uber for business purposes. I am therefore refusing your request for directives around the use of Uber under section 18(e) of the OIA, as the information does not exist.

If you disagree with my decision on your OIA request, you can ask an Inland Revenue review officer to review my decision. To ask for an internal review, please email the Commissioner of Inland Revenue at: CommissionersCorrespondence@ird.govt.nz.

Alternatively, under section 28(3) of the OIA, you have the right to ask the Ombudsman to investigate and review my decision. You can contact the office of the Ombudsman by email at: info@ombudsman.parliament.nz.

Thank you for your request.

Yours sincerely

George Fraser
Group Lead – Customer Interaction

Inland Revenue
Te Tari Taake

16 December 2019

s9(2)(a)

Dear s9(2)(a)

Thank you for your request made under the Official Information Act 1982 (the OIA), received on 4 October 2019. You requested the following:

> *Can you please tell me if Pornhub.com has been visited by staff between August 2018 and August 2019. Please provide the number of times staff have accessed, attempted to access or been blocked from accessing the site.*
>
> *Please include a breakdown of the number of times it was visited and the number of times an attempt was blocked by month.*
>
> *Please also include details of other sites staff have attempted to access that have been blocked including site names, dates and number of attempts.*

On 4 November 2019, the time limit for making a decision on your request was extended by 30 working days to 16 December 2019.

Inland Revenue uses third-party vendor services which utilise internet blocking software to block access to a large number of categories of predefined sites. Responding to your request required restoring from backup archived data from these third-party vendors. Information from 1 August 2018 to 31 October 2018 was not able to be recovered. Accordingly, I am refusing your request for information for this time period under section 18(e) of the OIA, as the information requested does not exist.

For the time period 1 November 2018 to 31 August 2019, there were two attempts by staff to access the Pornhub.com site, once in March 2019 and once in August 2019. Both of these attempts were blocked. An authorised attempt, which was blocked was undertaken in March 2019 to verify the internet blocking rules in place.

In regard to the last part of your request, Inland Revenue employs a large number of staff and the internet blocking software utilised by our third-party vendors blocks a wide range of predefined sites, including automatic access attempts made by website advertisements, pictures, links and scripts, of which the user may be unaware. Inland Revenue is confident that regardless of the number of access attempts no staff member was able to access any of these blocked sites.

Providing details of blocked attempts to other sites for the same timeframe would require a significant amount of resources to process. Accordingly, I have decided to refuse your request under section 18(f) of the OIA, as the information requested cannot be made available without substantial collation.

Right of Review

If you disagree with my decision on your OIA request, you can ask an Inland Revenue review officer to review my decision. To ask for an internal review, please email the Commissioner of Inland Revenue at: CommissionersCorrespondence@ird.govt.nz.

Alternatively, under section 28(3) of the OIA, you have the right to ask the Ombudsman to investigate and review my decision. You can contact the office of the Ombudsman by email at: info@ombudsman.parliament.nz.

Thank you for your request. I trust that the information provided is of assistance to you.

Yours sincerely

Gary Baird
Chief Technology Officer

Inland Revenue
Te Tari Taake

Corporate Integrity and Assurance
Corporate Risk and Assurance

30 June 2020

s9(2)(a)

Dear s9(2)(a)

Thank you for your request made under the Official Information Act 1982 (the OIA), received on 2 June 2020. You requested the following:

> *Details of all monitoring/productivity measuring software/tools used to monitor staff of the department, including when it came into effect, what it's purpose is, and any policy documents related to the software.*
>
> *This includes information on any free trials/trial periods of use of such software/tools for the last two years.*
>
> *Please confirm if the software is used for all staff, office staff only, or remote workers only.*

Inland Revenue has systems in place to monitor all staff internet usage on Inland Revenue systems, which is monitored and reviewed if necessary.

Inland Revenue maintains full audit logs and has various rules in place to monitor specific types of activity. If necessary for an investigation, we can tell what documents have been opened, copied, e-mailed, modified, or deleted.

Our tax system, START, logs exactly what information is accessed.

Our Code of Conduct and Use of Business Tools policies make it very clear that Inland Revenue tools are only to be used lawfully and appropriately, and that the use of these tools is monitored. Inland Revenue also has specific legislation that requires us to manage the access to and use of tax information, and to protect the integrity of the tax system (sections 6 and 18 of the Tax Administration Act 1994).

The Code of Conduct and the Use of Business Tools policy are attached to this response.

I cannot provide you with the name of the software Inland Revenue uses as to do so may negatively impact the integrity of the tax system as making the requested information available would be contrary to the provisions of a specified enactment, namely Inland Revenue's confidentiality obligation in section 18 of the Tax Administration Act 1994 (TAA). Disclosure of this information does not fall within any of the exceptions to the confidentiality obligation listed in sections 18D to 18J of the TAA.

Right of Review

If you disagree with my decision on your OIA request, you can ask an Inland Revenue review officer to review my decision. To ask for an internal review, please email the Commissioner of Inland Revenue at: CommissionersCorrespondence@ird.govt.nz.

Alternatively, under section 28(3) of the OIA, you have the right to ask the Ombudsman to investigate and review my decision. You can contact the office of the Ombudsman by email at: info@ombudsman.parliament.nz.

Thank you for your request.

Yours sincerely

Chris Linton
Manager Integrity Assurance

Next page >

Inland Revenue

Our Code
Tikanga Whanonga

Inland Revenue
Te Tari Taake

Inland Revenue
Code of Conduct
2019

doing the right thing...

Contents

Our Code of Conduct (Tikanga Whanonga) has the State Service Standards of Integrity & Conduct at its core (section 2). It also has more detail on topics particularly relevant to us all at Inland Revenue (IR) (section 3).

Making expectations clear

Everybody working for IR needs to be clear on the expected standards of behaviour.

Our Code is intended to help you do the right thing and guide you in your day-to-day decision making. It's all about making sure you know what is and isn't OK.

Doing the right things as individuals and as an organisation helps support a positive work environment and ensures the public and government have trust in IR and the tax system.

Helping you to make the right decisions

While our Code summarises the essential expectations, it doesn't cover every possible requirement or situation. It provides principles, standards and tools to help you decide whether an action is appropriate.

Our Code recognises and builds on the foundation principles for employment (already in our employment agreements) and relevant legislation. IR's policies, guidelines, frameworks and processes reinforce our Code and provide more detail when needed.

We all need to exercise good judgement in the decisions we make. Use the Making the right decision checklist on the next page to help you.

If you are uncertain about the right course of action, discuss any issue with your leader and seek their guidance.

Realising our vision, living our values and shaping our culture

Acting in ways consistent with our Code helps us achieve our vision, puts our values into practice and shapes our culture.

Most New Zealanders interact with IR in some way. Our success is built on the commitment, behaviours and spirit of service we demonstrate when delivering our services to the community.

The trust of our customers and the wider public is key. It's built on the good decisions we each make, the standards of integrity and conduct we maintain and the way we treat our customers.

It's our Code and we're all responsible

Our Code applies to everyone working for IR, in all roles and at all levels. As well as employees, it also covers agency staff, contractors and consultants. As the ways we work and the places we work change, it's important to remember that our Code will always apply and guide you.

We all have a role in ensuring our judgement, choices and actions, and those of our colleagues, uphold our reputation, make IR a great place to work, and are fair, impartial, responsible and trustworthy.

Making the right decision checklist

Acting with integrity involves making decisions that are inherently sound. This includes using good judgement and a logical process of thinking about whether your conduct and actions are appropriate to the situation.

Common sense and good judgement based on well-reasoned decision making will help you sensibly apply our Code to any situation you face. If you are unsure if your decision is OK ask yourself these checklist questions:

Remember: if it doesn't feel right it probably isn't!

If you are not sure what is an appropriate response to a situation, you must discuss the issue with your leader before taking any action. Similarly, if you think others may not be making good decisions or are behaving inappropriately, please speak up.

For further support refer to the specific policies and guidelines which relate to your decision, and if appropriate consider HR and financial delegations.

Is it legal

Does your proposed action or decision comply with NZ law and IR policies? Is there any likelihood that your proposed action is against the law?

Is it fair?

Will the proposed action or decision be the same for someone else in the same circumstances? Is it consistent with previous actions or decisions you have made or others have made? Will it give you or someone else an unfair advantage or benefit?

Is it free from any bias?

Are you being impartial and open-minded? Do you have a preconceived or unreasoned view of the situation that may be influencing your thinking in some way?

Is it likely to be misunderstood?

Consider the public's perception of your proposed action or decision. Could there be an unfavourable or adverse reaction because you have not been clear in your logic or reasoning?

Is it open to scrutiny?

Are your stated reasons for taking the proposed action your real reasons? Do you have an ulterior motive? Can you explain your logic and your action to others? Will it stand up to close examination or inspection and would you be comfortable if it appeared in the media?

Is it sensible?

Does it make good sense? Is it logical and well-reasoned? Have you thought through any potential risks and taken appropriate steps to avoid them or manage them effectively?

2. State Service Standards of Integrity & Conduct

We must be fair, impartial, responsible & trustworthy.

STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

The State Services is made up of many organisations with powers to carry out the work of New Zealand's democratically elected governments.

Whether we work in a department or in a Crown entity, we must act with a spirit of service to the community and meet the same high standards of integrity and conduct in everything we do.

We must comply with the standards of integrity and conduct set out in this code. As part of complying with this code, our organisations must maintain policies and procedures that are consistent with it.

For further information see:
www.ssc.govt.nz/code

Fair

We must:

- treat everyone fairly and with respect.
- be professional and responsive.
- work to make government services accessible and effective.
- strive to make a difference to the well-being of New Zealand and all its people.

Impartial

We must:

- maintain the political neutrality required to enable us to work with current and future governments.
- carry out the functions of our organisation, unaffected by our personal beliefs.
- support our organisation to provide robust, unbiased advice.
- respect the authority of the government of the day.

Responsible

We must:

- act lawfully and objectively.
- use our organisation's resources carefully and only for intended purposes.
- treat information with care and use it only for proper purposes.
- work to improve the performance and efficiency of our organisation.

Trustworthy

We must:

- be honest.
- work to the best of our abilities.
- ensure our actions are not affected by our personal interests or relationships.
- never misuse our position for personal gain.
- decline gifts or benefits that place us under any obligation or perceived influence.
- avoid any activities, work or non-work, that may harm the reputation of our organisation or of the State Services.

There's more detail on these standards, and the 18 expectation statements, in the SSC guidance document on the SSC website. There is also a te reo Māori version.

3. Helping you do the right thing at IR

We're all bound by the State Service Standards of Integrity & Conduct, which provide the foundation for our Code.

Our Code also expands on some critical areas to ensure that you know what's required in the IR context, which includes the unique role we have in administering New Zealand's Tax and Social Policy.

You must always maintain appropriate standards of professionalism. For example, coming to work when you're supposed to, being dressed appropriately, and performing your duties efficiently and safely are all part of what it means to be professional.

If in doubt, check it out!

- If you are in any doubt about what's OK and what's not, discuss it with your leader.
- **Use the Making the right decision checklist** to help you think it through.
- Sometimes mistakes happen. If you make a mistake you need to talk to your leader straight away.

We must maintain the integrity of the tax system, including ensuring information is protected and confidentiality maintained

The Tax Administration Act 1994 (TAA) sets out some specific obligations on those working for IR. These are critical to ensuring that the Government and public of New Zealand maintain trust in the tax and social policy systems IR administers.

These legal obligations require you to do your best to protect the integrity of the tax system, which includes taxpayer perceptions of integrity (section 6, TAA) and to keep IR information confidential (section 18, TAA).

Maintaining high standards of integrity and conduct ensures we all meet our legal obligations.

It's not part of your duties to access (or try to access) or change any IR customer information relating to your family, friends, acquaintances or yourself, using any access or authority IR has given you as part of your employment.

This is always unauthorised, regardless of the reason for doing so (like a customer's request, curiosity, just to change an address, just trying to help) or the degree of access (such as tried and the system prevented it, accessed but didn't modify). You also can't ask a colleague to undertake these actions for you, or take these actions at the request of your colleague/s.

Protecting the integrity of the tax system and meeting confidentiality requirements means you must only access customer information for the purposes of carrying out your IR duties.

You can refer a family member, friend or acquaintance only to information that is publicly available, including directing them to IR's website, myIR or our contact centre. Likewise, as an IR customer, you can use these publicly available channels including myIR for your own tax affairs.

For more details refer to our guidelines on Providing assistance to family, friends and acquaintances in our **People Policies & Guidelines**. This includes a definition of friends and acquaintances, examples and some specific considerations for certain IR roles which actively service the community.

We must treat all IR work with care and confidentiality, taking reasonable care to ensure IR information is accessible only to authorised people who have an IR business need.

No matter where you're working, whether within IR offices or off the premises, you must always ensure that IR information, in any form, is appropriately cared for, protected and secured, so it can't be seen or heard by unauthorised people or those without an IR business need (such as tradespeople working at your site or at home, or fellow passengers if you're working while travelling or commuting).

You must respect the privacy rights of our customers when dealing with their information. Only collect information you actually need, keep it secure, ensure it's accurate, and only use and disclose it lawfully. If dealing with requests to release information, you must follow specific IR procedures. You also need to ensure the confidentiality of all official information (including staff information).

We must use knowledge and influence gained at IR solely for appropriate business purposes.

Working for IR means you may have access to, and knowledge of, laws, procedures, activities and systems which could personally benefit you and others. You must use this knowledge – and the influence it may give you – only for appropriate IR business purposes and in ways that are open to the closest scrutiny.

You must not use any knowledge gained through your role at IR for your own, or anyone else's, advantage (financial or otherwise). You can only disclose IR information if you are authorised by IR to do so. This confidentiality requirement continues even when you stop working for IR.

Unacceptable use of knowledge and influence includes:

- telling a friend there are particular areas of business accounts which are scrutinised and audited more closely by IR
- giving information or assistance to an extended family member on how to deal with a dispute about tax, child support or a student loan, beyond what is publicly available
- using your role at IR to gather information not normally available to you as a member of the public, such as use of an IR warrant to obtain records of a business you or an acquaintance are interested in purchasing or looking them up in IR's systems.

We must avoid any actual, perceived or potential conflict of interest or preferential treatment

We're required to remain impartial and have the highest standards of integrity in any situation where an actual, perceived or potential conflict may arise. It's important these are identified, disclosed and managed appropriately as soon as you become aware of them.

You must discuss any potential issue with your leader before taking any action. This is to protect you and IR from possible criticism or compromise.

For more details, refer to the Disclosure & conflict of interest policy and guidelines in our **People Policies & Guidelines**. Also see the SSC guidelines. In relation to buying decisions, refer to **IR's probity framework for procurement.**

We must consider whether other activities (including paid and unpaid work) could conflict with or compromise our IR duties, affect our performance, or create an integrity issue.

It's important to discuss any other work outside of IR with your leader, to avoid any conflict. For all paid, and unpaid work (such as voluntary roles) which might create a conflict, you will also need your leader's written agreement before you start.

IR has specific requirements for providing assistance to clubs, societies and similar organisations, and being a nominated person who acts for someone else's tax affairs.

The Disclosure & conflict of interest guidelines include some examples of activities which could cause a conflict of interest and need to be discussed with your leader.

Examples of activities which could cause a conflict of interest:

- being an employee, advisor, director or partner of another business or organisation
- undertaking independent contracting or consultancy work
- running your own business, or helping your partner or family run a business
- being treasurer for a sports club
- auditing or considering an adjudication or ruling in relation to a company in which you own shares.

For more details, refer to the Disclosure & conflict of interest policy and guidelines, and also specific guidelines on Providing assistance to clubs, societies and other like organisations, and Becoming a nominated person, in our **People Policies & Guidelines**.

We must decline gifts or benefits that place us under any obligation or perceived influence.

As a general rule it is safer and simpler to refuse any gift offered to you as part of working for IR. The acceptance or soliciting of gifts, prizes, fees, entertainment, hospitality or any other form of reward may be, or could be seen to be, an inducement that puts you under an obligation to another party.

At certain occasions cultural traditions require the exchange of gifts, for example at a hui. In these situations, gifts can be accepted in line with IR's policy.

For more details and examples refer to the Gifts and hospitality policy (which includes the requirement for registering gifts, even if declined), Koha policy and Travel policy on **IR's Policy page.**

We must ensure our own tax affairs are beyond reproach

You have the same rights and responsibilities as any other IR customer. However, as you work for IR your tax affairs (personal and any business) must be beyond reproach, and you must comply with all the legislation we administer.

This includes accurate and timely tax returns and payments (or ensuring they are under arrangement by the due date), paying correct child support and/or student loans, and correctly claiming Working for Families Tax Credits. You must not omit income or evade tax in any way or encourage anyone else to do so, such as by accepting or requesting cash jobs.

IR understands that you might not always get it right or that you may disagree on a particular tax issue. If this happens, you need to engage with IR promptly and work through the proper channels to resolve the issue.

Our business tools support us in doing our jobs effectively - we must always apply good judgement in their use

Our Use of business tools policy and guidelines explain personal use, inappropriate material, inappropriate use, care and security, and monitoring. In general, you must consider what is legal, ethical and sensible, and ensure any use doesn't bring IR into disrepute or put IR funds, information or property at risk.

For more details refer to the Use of business tools policy and guidelines in our **People Policies & Guidelines**. Our guidelines also provide links to other related material. Also see the SSC guidelines.

We must all contribute to an inclusive, respectful, safe and healthy workplace

IR is committed to maintaining a safe and positive working environment and culture. This means we must all respect the rights of our colleagues and customers.

- Working in a safe and healthy way is what we do. We all contribute to maintaining a healthy and safe workplace and must take responsibility for our own health and safety.
- Everyone is respected and valued. We all support an inclusive workplace and value diversity of thought, beliefs, backgrounds and capabilities.
- Discrimination, bullying, harassment and violence of any kind are unacceptable.

It's important that everyone feels safe and supported to speak up about any issue.

For more details refer to the H&S commitment, Diversity policy, and Discrimination, harassment and bullying policy and guidelines in our **People Policies & Guidelines**.

We must be mindful of the appropriateness of any private or public comment

Generally, while working for IR you have the same rights of free speech and independent action as all New Zealanders. But you also have a duty to ensure any comments you make don't discredit or have the potential to discredit IR, the wider state sector or the Government.

Be aware of the perception of comments you make and ensure it's clear that when you are commenting as a private individual, you are sharing your personal view and not acting as a representative of IR. If you are in a senior or high-profile role, it may be difficult for you to separate your personal views from public perception of you as an IR representative.

Only specifically authorised staff can comment on IR matters or release IR material to any member of the media or public, or other organisation. Media includes anything that is being published or broadcast, such as via internet or social media channels, radio and television, newspapers, magazines and community newsletters.

Remember, you must treat all information, including knowledge of internal systems and processes gained while working for IR with care and confidentiality. This requirement continues even when you stop working for IR.

We must maintain the political neutrality required to enable us to work with current and future governments

Political neutrality and the perception of that neutrality is fundamental to the New Zealand Public Service. You must be impartial and always perform your role in a politically neutral way.

You must ensure no comment, decision or action undermines or could be perceived to undermine the government of the day or future governments or suggests any political preference or intent to influence other's political persuasion.

Please speak up – we're all responsible for reporting misconduct or wrongdoing

If you genuinely believe someone working for IR could be breaching our Code, acting unethically, or is (or has been) involved in wrongdoing – please speak up.

No matter how big or small, it's important that you raise your concerns.

Your first step is generally to speak to your leader. However, if you don't feel confident doing this you can contact the Integrity Assurance team who can support you with any concerns you have about coming forward. You can call or email them confidentially or use the **online reporting wrongdoing tool.**

If you are aware of serious wrongdoing, you may want to make a protected disclosure (this is sometimes called whistleblowing). Follow the **Guidelines for making a protected disclosure**, which explain what you need to do and how you are supported by the Protected Disclosures Act 2000.

For more details on reporting misconduct or wrongdoing, and for leaders, if you receive a complaint of wrongdoing or a protected disclosure, follow the steps in the **Managing misconduct and wrongdoing policy.**

Breaches of our Code may result in disciplinary action

Our Code is intended to help you understand the minimum expectations of behaviour at IR. Most people exercise good judgement and do the right thing. Being clear on expected behaviours and highlighting the very serious consequences of certain breaches, helps us all avoid breaches as much as possible. IR monitors various staff activity and practices to ensure alignment with policy and our Code.

A possible breach of our Code may result in an investigation and disciplinary action. Each matter will be considered on its own merits and the principles of natural justice will apply. These include an unbiased and fair process and the opportunity for an advocate or support person to be involved.

The action taken will depend on the severity of the breach and can range from warnings to dismissal in cases of serious misconduct, and in some situations, prosecution as well. Any person who knowingly breaches their confidentiality obligations under the TAA may be prosecuted and face penalties of imprisonment or a fine, or both.

Dismissal can result from serious breaches of our Code, such as:

- Accessing (or trying to access) and/or changing any IR customer information relating to your family, friends, acquaintances or yourself, using any access or authority IR has given you as part of your employment
- Accessing (or trying to access) and/or disclosing any IR information without IR authority
- Breaching confidentiality obligations under the TAA
- Falsifying tax returns or documents
- Dishonest, illegal or corrupt behaviour in the workplace
- Misusing IR property, business tools, business platforms or funds
- Accessing, downloading, and/or storing material from inappropriate internet sites or sending or receiving inappropriate material
- Knowingly, negligently or carelessly subjecting IR assets and resources to undue risks
- Harassment, discrimination or bullying against any colleague or customer
- Violence in the workplace
- Taking illegal drugs or consuming alcohol or other substances that affect your ability to perform your duties
- Behaviour that is likely to bring IR or the public service into disrepute

Inland Revenue
Te Tari Taake

Inland Revenue
Te Tari Taake

Topic 3 – Conduct & behaviour

Kaupapa Whakamahi Taputapu

Use of Business Tools Policy

This policy explains Inland Revenue's expectations in relation to the use of business tools for both business and personal use.

Note: Refer to the Vehicle and Parking Policy for information covering the use of motor vehicles.

In the normal course of work at Inland Revenue our people are entrusted with a range or business tools which help them do their jobs effectively.

The business tools at our disposal are hugely varied and include a mixture of physical tools and equipment as well as the systems and networks we have access to.

Business tools are there to be used and are a key part of our everyday business operations. We want to empower our people to tap into the practical value of business tools and use these resources to optimum effect.

Why we have this policy

This policy looks to ensure our people are clear on Inland Revenue's expectations in relation to using business tools.

Our Code of Conduct (you can find a copy in our People Policies & Guidelines) requires our people to 'use our organisation's resources carefully and only for intended purposes'. We must apply good judgement around business tool use and consider what is legal, ethical and sensible and ensure any use doesn't bring Inland Revenue into disrepute or put Inland Revenue's funds, information, or property at risk.

Who this policy applies to

This policy, and the guidelines which support them, apply to all Inland Revenue employees and contracted individuals.

What happens if you do not comply with this policy?

Inland Revenue monitors its business tool use to ensure responsible and lawful use in line with this policy and Code obligations. Failure to meet and/or maintain the standards could have disciplinary consequences as set out in our Code of Conduct.

IF IN DOUBT, CHECK IT OUT:

If you are in any doubt about what's okay and what's not, discuss it with your leader. You can use the *Making the Right Decision Checklist* in our *Code of Conduct* to help you think it through.

Sometimes mistakes happen. If you make a mistake or end up accessing something by accident you need to raise that with you leader straight away.

Specific practice around use of business tools

PERSONAL USE

Inland Revenue allows occasional and moderate personal use of some business tools. Common examples are phones, internet, email etc. Personal use must not put Inland Revenue at risk, e.g. reputational damage, security and privacy breaches.

We trust our people to make sensible decisions around using business tools for personal reasons and to seek leader approval and direction as needed. In many cases this approval need not be sought on each individual occasion, but may take the form of a more general pre-approval around what reasonable personal use can be accommodated in your role (see our 'Use of Business Tools Guidelines' in our People Policies & Guidelines for more detail).

At Inland Revenue there are some clear exceptions where any personal use is strictly prohibited. It is never appropriate to access systems holding tax secret information (e.g. FIRST, START) or confidential employee or financial information (e.g. in payroll, finance, self-service tools etc.) unless it is for a legitimate business reason. Accessing these systems for personal or unauthorised reasons is in breach of our Code of Conduct and this policy and may amount to serious misconduct and/ or a criminal offence.

INAPPROPRIATE MATERIAL OR USE

Use of any business tools to access, download and/or store material from inappropriate, indecent or offensive internet sites or other sources is strictly forbidden, as is sending or knowingly receiving such material. Inappropriate sites and material include pornographic, provocative or distasteful images/text, and sexist, racist or otherwise offensive material. It is a criminal offence to intentionally cause harm by sending or posting digital communications (cyberbullying).

CARE AND SECURITY

Our people are responsible for the proper care and security of business tools in their possession (both in Inland Revenue offices and outside of them) including taking all reasonable precautions to prevent damage or loss and ensure confidentiality of Inland Revenue information.

The Tax Administration Act requires taxpayer and tax related information be stored on approved systems. Only those Internet Cloud Systems which have been through a formal assessment and approval process can be used.

Our people must never share their passwords or allow any other person to use their ID or passwords for any reason. Non-Inland Revenue people, such as friends and family, must not use Inland Revenue business tools.

BRING YOUR OWN DEVICE (BYOD)

Note: Inland Revenue is increasingly promoting the use of (BYOD) Bring Your Own Device technologies. While this policy does not extend to include these devices (as they are not supplied by Inland Revenue), we ask that our people apply appropriate judgement around the use of non-Inland Revenue technology for work purposes, and that they don't place themselves or Inland Revenue at risk through inappropriate use.

Our people should be mindful that if they are using their own device for work purposes (either at home or in the office) interaction with Inland Revenue's systems, information or use of our technology through their device is still covered under this policy and our Code of Conduct.

Document control	**v1**, **Sept 2019** *(this content was a section within a previous Conduct & behaviour policy)* (minor edits and reformat Sept 2019)
Review dates	September 2021
Policy owner	Employment Relations, Policy & Remuneration Manager, People & Culture
Policy contact	Email the ERP&R team

Inland Revenue
Te Tari Taake

27 August 2020

s9(2)(a)

Dear s9(2)(a)

Thank you for your request made under the Official Information Act 1982 (the OIA), received on 27 July 2020. You requested the following:

> *...internal memoranda and other documents, including legal opinions, that informed the IRD policy decision to define cryptocurrency as property for taxation purposes...Only documentation that was immediately relevant to the final determination is sought.*

On 24 August 2020, the time required to respond to your request was extended by 5 working days to enable necessary consultation.

Information being released

Please find enclosed the following documents:

Item	Date	Type	Title
1	N/A	Opinion	Bitcoin: Applying sections CA 1, BB 1 and LD 1 of the Income Tax Act 2007, and section 8 of the Goods and Services Tax Act 1985
2	2 October 2015	Policy research document	Tax Treatment of Bitcoin in New Zealand

Some information in Item 1 is withheld under section 9(2)(g)(i) to maintain the effective conduct of public affairs through the free and frank expression of opinions.

The enclosed documents also include information that is outside the scope of your request. This information has not been considered for release and has been removed from the documents or redacted as "outside scope".

The enclosed documents refer to the underlying thinking that informed the decision to treat cryptocurrency as property for tax purposes. While the research document was not directly relevant to the decision, the document made some suggestions of treatment, some of which were not ultimately adopted. This has been provided for completeness.

The reason for treating cryptocurrency as property and not money is set out succinctly in *PUB00323 Issues Paper number 11: Whether remuneration paid to an employee in cryptocurrency is subject to PAYE or FBT (20 June 2018*) as follows:

> [4.16] However, cryptocurrency is not "money" as commonly understood (at least not at the present time). In particular, because cryptocurrency is not issued by any government, it is not legal tender anywhere. Further, although acceptance of certain cryptocurrencies as payment for goods and services is increasing, it is not "generally accepted" as payment. Given the extreme volatility experienced to date, there are also issues around cryptocurrency's ability to be a store of value.

Ultimately, the decision was based on the fact that money is something that is generally accepted as payment, a store of value and is legal tender (i.e. a means of exchange issued by a government). As cryptocurrency is currently not money, it is considered to be personal property. We note that the industry is constantly evolving, and we are keeping an eye on recent developments.

Right of Review

If you disagree with my decisions on your OIA request, you can ask an Inland Revenue review officer to review my decisions. To ask for an internal review, please email the Commissioner of Inland Revenue at: CommissionersCorrespondence@ird.govt.nz.

Alternatively, under section 28(3) of the OIA, you have the right to ask the Ombudsman to investigate and review my decision. You can contact the office of the Ombudsman by email at: info@ombudsman.parliament.nz.

Thank you for your request. I trust that the information provided is of assistance to you.

Yours sincerely

Josh Green
Acting Manager
Government & Executive Services

Outside scope

6 LEGISLATION

GST: introductory principles

6.1 Section 8 of the GST Act imposes tax on the supply (but not an exempt supply) in New Zealand of goods and services by a registered person in the course or furtherance of a taxable activity carried on by that person.

Consideration

6.2 GST is levied on supplies of goods or services. The amount of tax levied is based on the value of the supply. The issue of valid consideration arises because it is the basis on which the value of the supply and thus the amount of tax levied is calculated.

[42] Staples Updating Master Tax Guide, para 34-025.

6.3 Section 2 of the GST Act defines "consideration" in relation "to the supply of goods and services to any person" as including "any payment made or any act or forebearance [...] in respect of, in response to, or for the inducement of, the supply of any goods or services [...]".[43] Although the term "payment" is used, the definition is intended to be broad in scope, encompassing payments in forms other than cash. This is evidenced by other sections of the GST Act, such as section 10(2)(b), which specifies how the value of a supply of goods and services is to be calculated "to the extent that the consideration for the supply is not consideration in money".[44]

"Goods and services"

6.4 As GST is charged on supplies of *goods and services*, it must be determined whether what is being supplied falls within the scope of these terms.

6.5 Section 2 of the GST Act defines "goods" as including "all kinds of personal and real property" other than "choses in action", which is further defined in section 2 as including "money".[45] The term "services" is defined as encompassing anything that is not goods or money.[46]

6.6 For the purposes of this opinion, the relevant part of the section 2 definition of "money" is the first paragraph, which reads:

> *(a) Bank notes and other currency, being any negotiable instruments used or circulated, or intended for use or circulation, as currency.*

6.7 In order to determine whether what is being supplied is "money" and therefore outside the scope of "goods and services" for the purposes of the GST Act, it must therefore be ascertained whether what is being supplied constitutes a "currency".

6.8 Section 3(2) of the GST Act defines "currency" as "any banknote", or other currency of any country, other than when used as a collector's piece, investment article, item of numismatic interest, of otherwise than as a medium of exchange". Paragraph 104.6.3.1 of the Technical Rulings Manual also notes the definition of currency provided in the Shorter Oxford Dictionary: "the circulating medium; the money of a country in actual use."

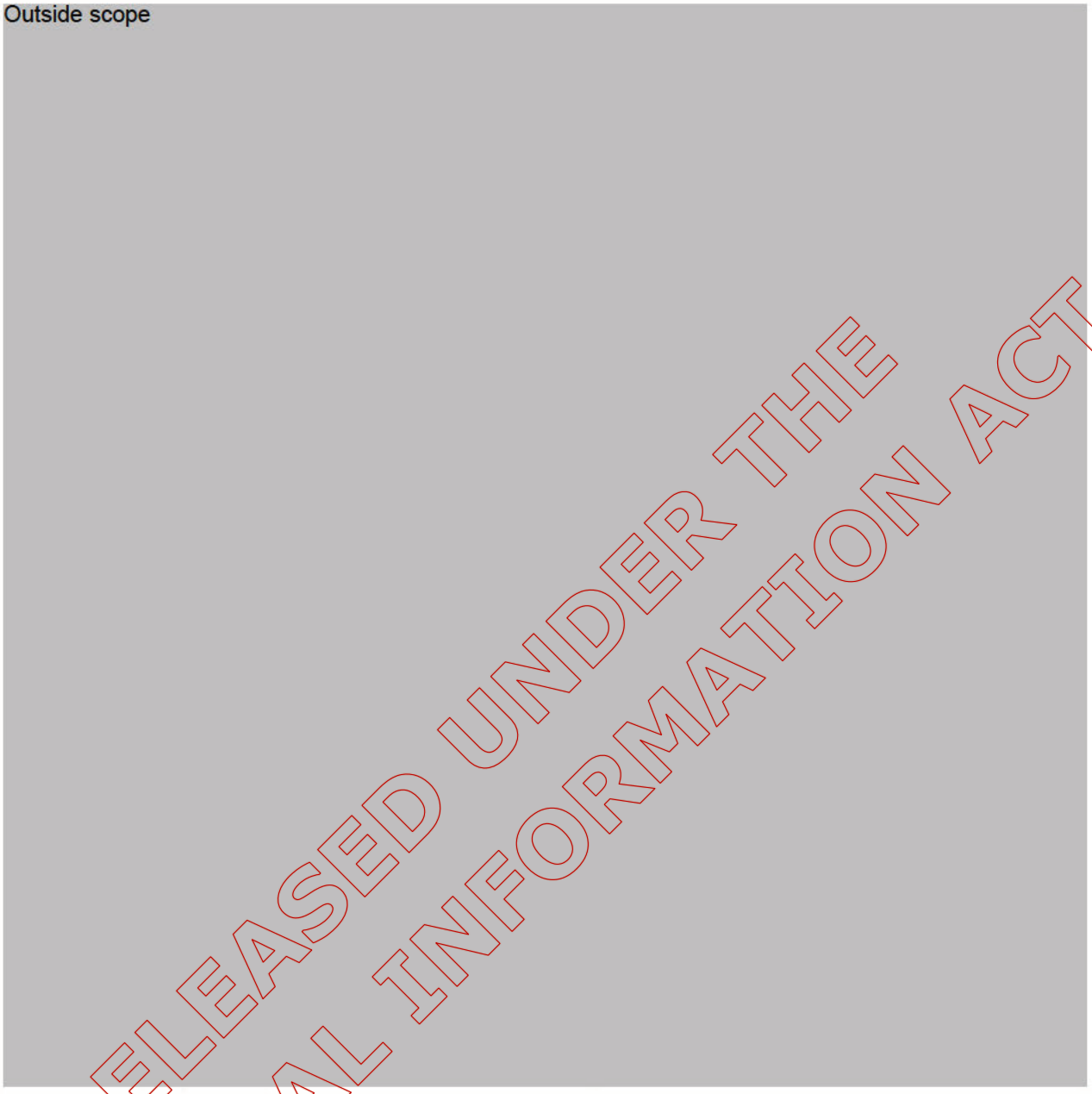
6.9 While the focus of these two definitions would appear to be whether the supply in question is a circulating medium in actual use, they both define "currency" as belonging to a specific country. That "currency" is tied to a particular sovereign territory, backed by a government authority, is further supported by the definition of currency in the New Zealand Law Dictionary: "[a] unit of money in use in a **country**".

6.10 Inland Revenue follows the OECD decision of treating products digitally supplied as services.[47]

---

[43] GST Act, s 2.
[44] GST Act, s 10(2)(b).
[45] GST Act, s 2.
[46] Ibid.

Outside scope



7 ANALYSIS

Consideration

7.1 As discussed above, the definition of consideration provided in section 2 of the GST Act is broad in scope, encompassing payments in forms other than cash. Bitcoins received in respect of goods and services supplied will therefore fall within the scope of the GST Act's intended meaning of "consideration".

[53] GST Act 1985, s 3(1)(a).

7.2 The conclusion that Bitcoins should be regarded as consideration for the purposes of the GST Act is supported by the Australian Tax Office's position on Bartercard credits and taxable supply. The Australian Tax Office has stated that where an entity belonging to a Barter scheme makes a supply satisfying the equivalent Australian requirements for a taxable supply, the crediting of the supplier's Bartercard membership account and the debiting of the receiver's membership account with Bartercard credits will constitute consideration for that taxable supply.[54]

7.3 Provided the other elements of section 8 of the GST Act are satisfied (i.e. there is a supply of goods or services, in the course or furtherance of a taxable activity, in New Zealand) and the transfer of Bitcoin credits is made *for* the goods or services supplied,[55] Bitcoins are valid consideration for the purposes of determining whether there is a taxable supply for the purposes of section 8 of the GST Act.

Do Bitcoins fall within the scope of "goods and services"?

7.4 As discussed above, the term "goods" is defined in section 2 of the GST Act as including "all kinds of personal and real property", but not "choses in action", which is further defined as including "money".[56] The term "services" is defined in section 2 of the GST Act as encompassing anything that is not goods or money.

7.5 "Money" is in turn defined as "bank notes or other currency [...] intended for use or circulation, as currency".[57] In determining whether Bitcoins fall within the scope of "goods and services" for the purposes of section 8, it must therefore be ascertained whether Bitcoin is regarded as a "currency".

7.6 As discussed above, currency is defined as a circulating medium *of* a particular country. While Bitcoin would appear to accord with the focus of section 3(2) of the GST Act and the Shorter Oxford definitions in that it is a circulating medium in actual use, it cannot be said to be the money of a specific country; indeed, one of the key characteristics of the Bitcoin medium of exchange is that it is "decentralized [...] not backed by any government or other legal entity".[58] If the concept of "currency" is limited to mediums of exchange authorised by the government authority of a sovereign territory, Bitcoins will not be regarded as "money" and can therefore fall within the scope of the term "goods and services" for the purposes of section 8 of the GST Act.

[54] Australian Tax Office, GSTR 2003/14, Goods and Services Tax Ruling.
[55] *NZ Refining Co Ltd v CIR* (1997) 18 NZTC 13,187.
[56] GST Act 1985, s 2.
[57] Goods and Services Tax Ac1985.
[58] Grinsberg, R. *Bitcoin: An Innovative Alternative Digital Currency*, Yale Law School, Dec. 9 2011, at 160.

7.7 A conclusion that Bitcoins do not meet the definition of "currency" and cannot therefore be regarded as "money" would be in line with the Australian Tax Office Goods and Services Tax Ruling 2003/14 on the GST implications of transactions involving Barter credits. The Ruling states that in the scenario of one member of a Barter scheme selling their credits to another member for cash, the supply of the credit in the other member's account would not be regarded as money, the transferring of the credit from the supplier entity's account to the recipient entity's account representing a "*supply* of the credit and not a *payment* for the cash received".[59]

7.8 As Bitcoins are therefore unlikely to be regarded as a currency, they are able to be caught by the scope of "goods and services" for the purposes of section 8 of the GST Act.

7.9 Where Bitcoins are supplied by the purchaser to the seller in their physical *coin* form, this will constitute a supply of goods.

7.10 As stated above, Inland Revenue follows the OECD decision of treating products digitally supplied as services. This means that where the entire transaction occurs over the internet and the Bitcoins are debited from the miner's digital wallet and transferred to the purchaser's digital wallet, the Bitcoins remaining in their digitalized form (as opposed to being traded in physical *coin* format), the digital Bitcoins will be regarded as services.

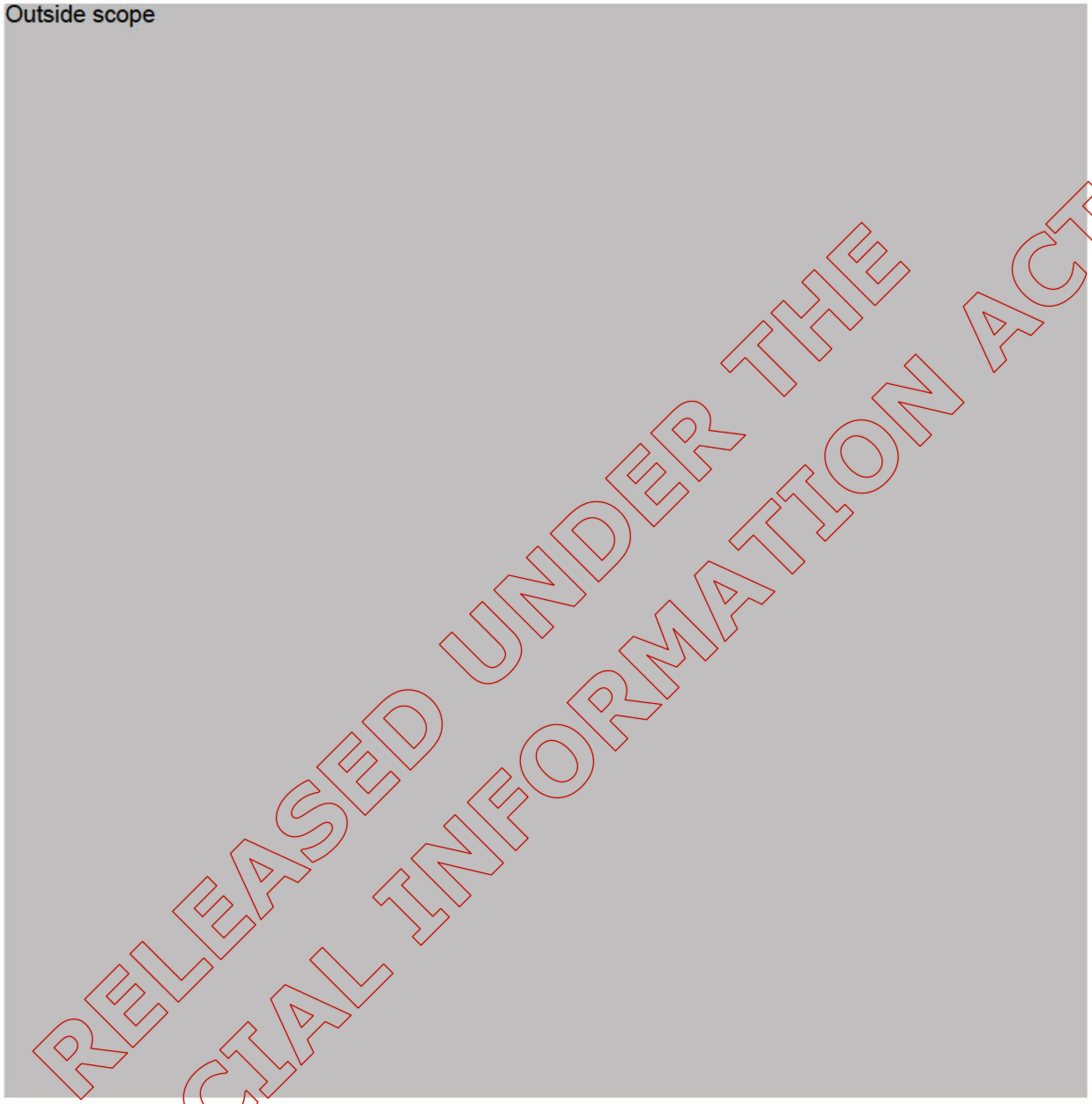
7.11 As a supply of Bitcoins will therefore constitute either a supply of goods – where they are transferred in their physical form – or services – where they are transferred over the internet – it is able to constitute a taxable supply for the purposes of determining liability to GST.

Outside scope

[redacted]

[59] Australian Tax Office Goods and Services Tax Ruling 2003/14.
[60] GST Act 1985, s 8(2).

Outside scope



Will transactions involving Bitcoins fall within the financial services exemption?

7.16 Even where a Bitcoin trade constitutes a taxable supply in New Zealand for the purposes of section 8 of the GST Act, the transaction will not be liable to GST if it is regarded as being a supply of financial services and therefore constitutes an exempt supply pursuant to section 14(1)(a) of the GST Act.

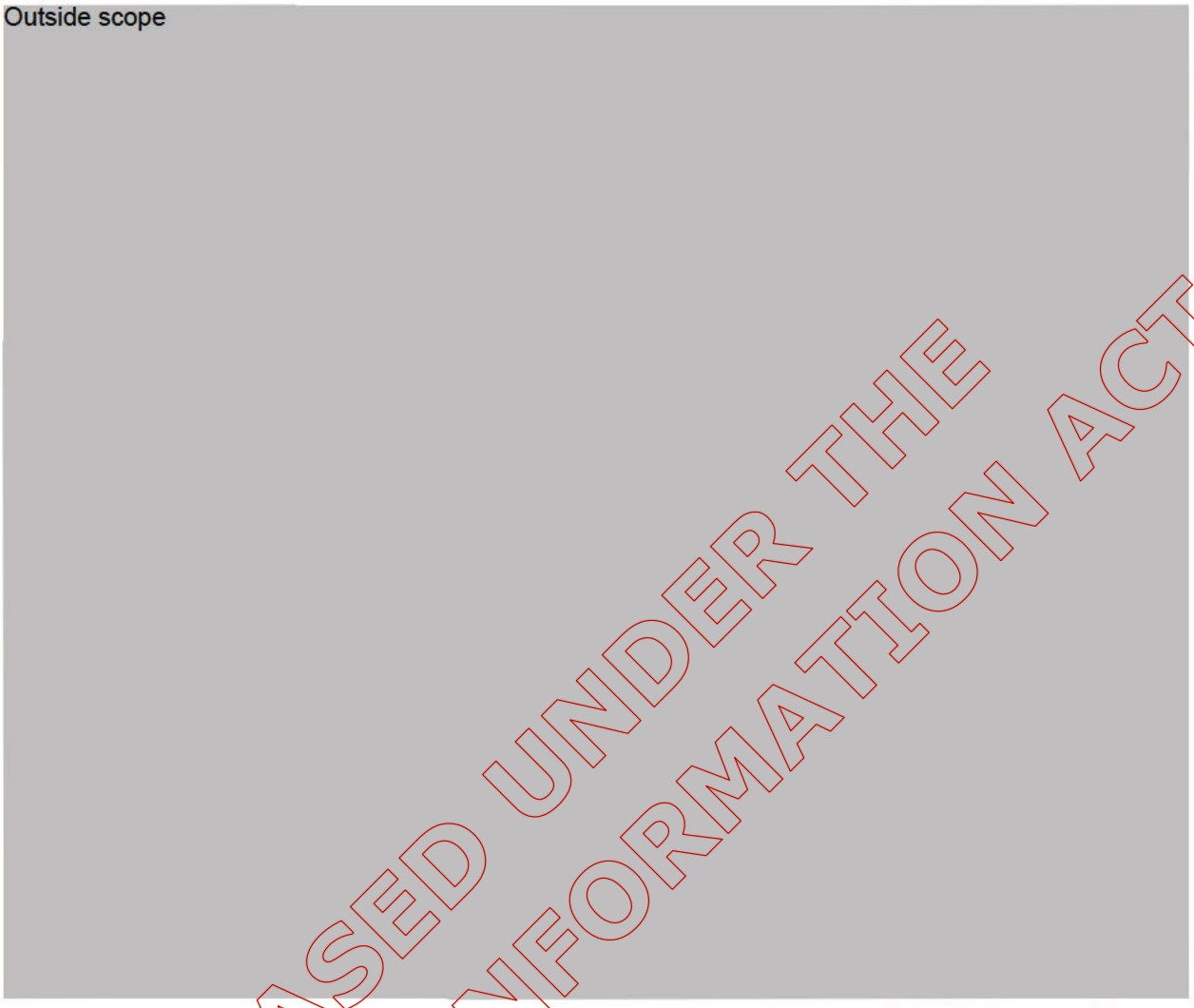
[61] GST Act 1985, s 3.

7.17 As discussed above, the question of whether the trade of Bitcoins falls within the scope of "financial services" as the concept is defined in section 3(1)(a) of the GST Act is dependent on whether the trade of Bitcoins are regarded as the "exchange of currency".[62] As it is unlikely that Bitcoins can be regarded as a currency, as they are not the medium of exchange *of a country*, Bitcoin transactions are unlikely to fall within the definition of "financial services" and will therefore not be caught by the exemption. Where the requirements of section 8 of the GST Act are met, trades involving Bitcoins will therefore be liable to GST.

Outside scope

[62] GST Act 1985, s 3(1)(a).

Outside scope



4. My research went beyond providing an interpretative view that fits within the existing framework. Rather my research took a first principles policy approach. After careful analysis of the characteristics and use of Bitcoin I recommend that Inland Revenue view Bitcoin as 'money' for GST purposes due to it serving as a medium of exchange, a unit of account and a store of value in a way similar to legal tender. s9(2)(g)(i) This would impose an increased obligation on the government to regulate the crypto currency market. Currently bitcoins are generally an unregulated alternative payment method or store of value. Without regulation consumers who transact in bitcoins are not protected against any adverse effects associated with Bitcoin transactions, such as hacking and theft.

5. Generally, the way bitcoin transactions are treated under the *Income Tax Act 2007* (ITA) will be similar to legal tender transactions for income tax purposes. The definition of 'money' in the ITA permits a very wide interpretation as it can include "money's worth"; this would include bitcoins. The various provisions in Part C of the ITA are designed to cast a wide net in order to catch a taxpayer's income as assessable. It is clear that income arising from Bitcoin transactions is income. This is important as the type of income impacts on how and when it is reported.

[1] Digital Currency: Recent Government Statements.

International Approaches

Verdicts have been reached by some international tax authorities regarding the taxation treatment of various transactions involved with crypto currencies while other jurisdictions have remained silent on the issue. Some have outright banned crypto currencies while others offer their guidance about the taxation of crypto currencies but none have attempted any regulation. Scheduler systems like Japan and many European countries where income is only taxable to the extent you can fit it into a specific schedule will be under a lot more pressure than global systems like the USA to offer guidance about Bitcoin[1].

United Kingdom:

HM Revenue and Customs quietly issued a brief in September 2014 concerning the tax treatment of activities involving Bitcoin and other crypto currencies. The brief clarifies the UK tax authority's position on the crypto currency and offers guidance for Bitcoin traders, exchanges, payment processors, and other Bitcoin service providers as well as Bitcoin miners. It also addresses how the UK tax authority views Bitcoin for value added tax, capital gains tax, corporation tax and income tax purposes.

VAT

The VAT treatment for crypto currencies adopted by the UK must be consistent with any treatment eventually implemented across the European Union. Any changes will not apply retrospectively.

Income received from crypto-currency mining activities will generally be outside the scope of VAT on the basis that the activity does not constitute an economic activity for VAT purposes because there is an insufficient link between any services provided and any consideration received. Income received by miners for other activities, such as for the provision of services connected with the verification of specific transactions for which specific charges will be made, will be exempt from VAT under Article 135(1)(d) of the EU VAT Directive as falling within the definition of 'transactions, including negotiation, concerning deposits and current accounts, payments, transfers, debts and other negotiable instruments. When crypto currencies are exchanged for the British pound or for foreign currency, no VAT will be due on the value of the crypto currency itself. Any charges made over and above the value of crypto currency for arranging or carrying out any transactions in a crypto currency will be exempt from VAT under Article 135(1)(d) as outlined above. However in all instances, VAT will be due in the normal way from suppliers of any goods or services sold in exchange for Bitcoin or similar crypto currency. The value of the supply of goods or services from which the VAT is due will be the sterling value of the crypto currency at the point the transaction takes place. Previously HMRC had classified Bitcoin as a taxable voucher, which would have meant that exchanges selling Bitcoins in the UK would have had to cover VAT costs by tacking on a 20% mark-up putting exchanges operating in the UK at a disadvantage compared with exchanges in other countries. This would make it uneconomical for traders to operate in the UK, simply driving the market offshore. It made more sense to exempt Bitcoin from VAT, which would also have the benefit of reducing the scope for VAT fraud[1].

Corporation Tax

The profits or losses on exchange movements between currencies are taxable. For the tax treatment of crypto currencies, the general rules on foreign exchange and loan relationships apply. Profits and losses of a company entering into transactions involving Bitcoin would be reflected in accounts and taxable under normal Corporation Tax rules.

Income Tax

The profit and losses of a non-incorporated business on Bitcoin transactions must be reflected in their accounts and taxable on normal income tax rules.

HMRC was praised by a number of exchanges for giving crypto currencies legitimacy, especially after the demise of Mt Gox. This recognition gives digital currencies hope for long-term success.

Australia

The Australian Tax Office (ATO) is keeping a close eye on Bitcoin and monitoring Bitcoin and other payment systems as part of its monitoring of developments for which there are tax consequences. In general, tax rules that apply to conventional commercial transactions also apply to transactions carried out through the Internet or with emerging payment systems, such as crypto currencies.

Sellers of goods and services who accept payment from new types of payment tokens such as Bitcoin they may still need to charge GST on these goods and services or include the income in their business tax return.

The Australian Tax Office (ATO) recently released a Goods and Services Tax Ruling explaining the Commissioner's view on the goods and services tax (GST) consequences of transactions involving the use of bitcoin. The Ruling considers whether bitcoin may involve 'money' and whether it is a 'financial supply'. In considering the GST consequences, the Ruling focuses on the requirement that there must be a 'supply for consideration' for there to be a taxable supply.

'Money' is defined to specifically include, amongst other things, 'currency' (whether of Australian or of any other country)[1]. The term 'currency' is not yet defined.

Is Bitcoin 'money' for GST purposes?

Money is defined in section 195-1 of the GST Act. The use of the term 'includes' in this section indicates something broader than what follows in the statutory definition. In order to determine whether bitcoin is money it is necessary to consider each of the specified items in the definition. Bitcoin is not a legally recognised universal means of exchange and form of payment by the laws of Australia or the laws of any other country. Therefore it is not a currency under paragraph (a) of the definition of 'money'. Bitcoin also does not meet the definitions of 'money' under paragraph b), c), d) nor e).

In the Commissioner's view, the use of the term 'money' is intended to prescribe fiat currency and those financial instruments and payment mechanisms which are denominated in, or relate directly to, fiat currency despite the definition of 'money' not being exhaustive. Paragraphs (a)-(e) strongly indicate that 'money' for GST purposes cannot extend beyond methods of payment that are denominated in fiat currency. Thus bitcoin is not 'money' for GST purposes in Australia.

ATO GST Ruling on Bitcoin

The final Ruling concluded that a transfer of bitcoin from one entity to another is a 'supply' for GST purposes. The supply of bitcoin is not a 'financial supply' under section 40-5. It is not a input taxed supply under paragraph 9-30(2)(b). Bitcoin is also not a 'foreign currency' for Australian tax purposes.

A supply of bitcoin is a taxable supply under section 9-5 if certain entrepreneurial requirements are met. A supply of bitcoin in exchange for goods and services will be treated as a barter transaction. People buying the crypto currency will have to pay 10% GST when they buy Bitcoin in Australia and will then be charged a further 10% on the goods and services they then buy with it.

Capital Gains Tax

Bitcoins and other crypto currencies is an asset for Capital Gains Tax purposes. There may also be capital gains tax consequences where you dispose of bitcoin as part of carrying on a business. However, any capital gain is reduced by the amount that is included in your assessable income as ordinary income[1].

Paying salary or wages in Bitcoin

Payments of salary and wages in Bitcoins constitute a fringe benefit and the employer is subject to the provisions of the Fringe Benefits Tax Assessment Act[1].

Mining Bitcoin

Where you are in the business of mining bitcoin, any income that you derive from the transfer of the mined bitcoin to a third party would be included in your assessable income. Any expenses incurred in respect to the mining activity would be allowed as a deduction. Losses you make from the mining activity may also be subject to the non-commercial loss provisions.

Bitcoin held by a taxpayer carrying on a business of mining and selling bitcoin, will be considered to be trading stock. You are required to bring to account any bitcoin on hand at the end of each income year.

GST is payable on the supply of bitcoin made in the course or furtherance of your bitcoin mining enterprise. Input tax credits may be available for acquisitions made in carrying on your bitcoin mining enterprise[1].

Bitcoin exchange transactions

Where you are carrying on a business of buying and selling bitcoin as an exchange service, the proceeds you derive from the sale of bitcoin are included in assessable income. Any expenses incurred in respect to the exchange service, including the acquisition of bitcoin for sale, are allowed as a deduction. Bitcoin held by a taxpayer carrying on a bitcoin exchange will be considered to be trading stock and you are required to bring to account any bitcoin on hand at the end of each income year.

GST is payable on a supply of bitcoin by you in the course or furtherance of your exchange service enterprise. Input tax credits are available for bitcoin acquired if the supply of bitcoin to you is a taxable supply.

If you have acquired bitcoin as an investment, but are not carrying on a business of bitcoin investment, you will not be assessed on any profits resulting from the sale or be allowed any

deductions for any losses made (however, capital gains tax could apply). However, if your transactions amount to a profit-making undertaking or plan then the profits on disposal of the bitcoin will be assessable income[1].

USA

Several of the world's largest economies have gone public with their opinions and views on the taxation and regulation of Bitcoins however initially the USA was quiet on the matter, possibly taking a 'wait-and-see' approach to determine whether special guidance is needed. It is not clear whether most crypto currency users are holding coins for speculative purposes or using them to purchase goods and services. It is still unclear whether crypto currencies are still going to be around in a few years' time. It will be unnecessary to commit resources and time to a project that may be more or less important in the future.

There are several questions the IRS deems it needs to consider in determining how Bitcoin and other crypto currencies should be classified for tax purposes. The first is whether Bitcoin is a currency for which arguments could be made for both sides as there is no clear definition of a currency under the tax code. Other question posed are whether bitcoin is property in an ordinary (inventory for sale in trade) or capital (stocks, bonds) sense which in turn depends on many factors: who holds bitcoins and why they acquired them. The IRS believes it is ultimately going to come down to a question of characterisation after which the general tax principles should follow. There shouldn't be a need for special rules for crypto currencies. It is clear that income arising from Bitcoin transactions is income, but it remains a question of what type of income is it and how and when one reports it[1].

On March 25th 2014 the IRS posted on their website saying they are opting to class crypto currencies as property. General tax rules that apply to property transactions will apply to transactions conducted in crypto currency i.e. they will be taxed the same way as shares and barter transactions. This means that:

- Remuneration paid to employees using virtual currency is categorised as wages and is taxable to the employee, must be reported by an employer, and are subject to federal income tax withholding and payroll taxes.
- Payments using virtual currency made to independent contractors and other service providers are taxable and self-employment tax rules generally apply.
- The character of gain or loss from the sale or exchange of virtual currency depends on whether the virtual currency is a capital asset in the hands of the taxpayer.
- A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property.
- When a taxpayer successfully mines crypto currency, the fair market value as of the date of receipt is includible in gross income.

Canada

Canada has posted a public statement about Bitcoin and when and how taxpayers should report them. Barter transaction rules apply where bitcoins are used to purchase goods and services. In a barter transaction between arm's-length persons, the value of whatever is received is at least equal to the value of whatever is given up. If a business sells goods and services in exchange for bitcoins that

business must report its income from the transaction in Canadian Dollars. GST would be applicable on the fair market value of the Bitcoins that were used to pay for the goods and services.
If a taxpayer mines Bitcoins in a commercial manner, the taxpayer's income for the year from such mining activity will be determined with reference to the property in the taxpayer's inventory at the end of the year[1]. When Bitcoin is bought and sold like a commodity any resulting gains or losses may be classified as income or capital depending on the circumstances[1].

Russia and Vietnam

Russia and Vietnam are two countries that have outright banned the use of crypto currencies. Russia outlawed bitcoins in early February 2014 due to concerns that they could be used for money laundering and financing terrorism. On February 27 Vietnam followed suit, announcing that trading in crypto currencies is illegal[1].

Poland, Finland and Estonia

All three have indicated that the use of bitcoin is taxable for VAT purposes, although the taxable base can differ. For example, Estonia treat bitcoin transactions as a service whereas Finland takes the view that a bitcoin should be regarded as a commodity instead of a currency[1].

Sweden

Sweden has taken a keen interest in the evolution of crypto currencies with their tax enforcement agency, Skatteverket, discussing the taxation consequences of digital currencies very actively. Skatteverket has noticed a slight increase in questions from the public in regards to the taxation treatment of crypt currencies, especially whether there is an obligation to pay GST when buying and selling Bitcoins and the tax treatment of earnings related to Bitcoin mining. The Swedish tax Authority resolved that in absence of the definition of currency in the VAT Directive leads to the interpretation of the term as a means of payment. Wording in the Directive indicates that the term currency is not linked to legal tender. On the basis of the following considerations:

- exchange of bitcoin requires similar requirements to intermediation of financial services;
- Bitcoins are a means of payment used in a similar way to legal tender;
- Bitcoin have strong similarities to electronic money.

The Swedish Tax Authority held that bitcoin transactions should be considered as transactions concerning currency referred to in Article 135.1. Letter (e)[1].

Singapore

The Inland Revenue Authority of Singapore (IRAS) has issued their opinion on crypto currencies. The IRAS has been closely monitoring potential taxation compliance risks associated with using crypto currencies by individuals and businesses. Individuals and businesses accepting payment in bitcoins are subject to normal income tax rules. Businesses that purchase and sell crypto currencies will be taxed on the profit arising from trading and mining. Some businesses that buy crypto coins for long term investment might earn a capital gain upon disposal, however in Singapore there is no capital gains tax so no tax will be due.

Regarding GST treatment, in Singapore, crypto currencies are not considered currency, money or goods; instead the supply of crypto currencies is treated as a supply of services, which does not qualify for a GST exemption. If crypto currencies were used to pay for goods and services, such transactions are classified as barter trades thus GST would be charged if both the supplier and customer are registered for GST purposes. However, if a customer uses bitcoins to pay a supplier outside Singapore, the customer does not have to charge GST because the supply would be zero-rated.

A GST business selling bitcoins outright would also need to charge GST on those sales, unless it is a sale to a customer outside Singapore. If the business acts as an agent for another party, GST must be charged on the commission fees it receives, unless the service is supplied to a customer outside Singapore[1].

Germany

The German Federal Ministry of Finance has taken a slightly different approach to that of Singapore. They have given Bitcoin a legal status, recognising Bitcoin and other crypto currencies as a 'unit of account', comparable with foreign exchange accounting units that are not legal tender. It is not classified as e-money or a foreign currency but rather a financial instrument under German banking rules. Germany considers Bitcoin VAT exempt pursuant to point c in Article 135.1 d Directive 2006/112/EC on the basis that the mere payment does not constitute the provision of the service and therefore is not subject to VAT. Germany views Bitcoin as a financial instrument similar to 'private wealth' and Bitcoin mining amounts to private money creation, whose profits are subject to a capital gains tax of 25% unless they are held for more than a year. A member of the German Parliament's Finance Committee, Frank Schaeffler, believes that in a free country the government should not resist or intervene with citizen's private choice of money so will thus not be banning the crypto currency.

Norway

The Norwegian Directorate of Taxes published a statement in November 2013 explaining that Bitcoins are assets liable to tax. The department has not and cannot make a decision on whether Bitcoin is a currency. Profits from trading Bitcoins are liable to a tax of 27% and losses from trading can be deducted just like profits from the trade of other assets. Bitcoins owned at the end of the year are taxable under the wealth tax as assets valued to the market prices in Norwegian Krones at the end of the year.

Businesses that sell Bitcoin will be liable for 25% VAT on turnover as this supports the tax administration's view that Bitcoins are electronic services and not financial services, which are exempt from VAT[1].

Japan

Japan's government reportedly announced plans that it would set the rules for trading Bitcoin and impose taxes on the digital currency. The government will call for taxing of all Bitcoin transactions, purchases made with Bitcoin will be subject to an 8% consumption tax beginning April 1st 2014 and trading gains as well as corporate revenue arising from Bitcoin related transactions will also be subject to tax[1].

India

Indian is set out at taking a closer look at crypto currencies before issuing any guidance on the matter. In late December 2013 Indian tax officials visited CoinMonk Ventures, a Bitcoin mining start-up, to discuss how miners and Bitcoin businesses may be taxed. The Bitcoin community in India is willing to collaborate with and accommodate the government to ensure legal and tax treatments exist[1].

Switzerland

The Swiss Federal Tax Administration issued a statement saying that no guidance has been issued yet to taxpayers completing transactions in crypto currencies but noted that based on current laws it is possible to determine taxation of income in digital currency or regarding the value added tax[1].

Summary

With different countries offering varying guidance and regulations relating to crypto currencies it opens up the possibility of tax arbitrage (buying and selling securities, commodities and currency in different markets to take advantage of the differing prices for the same asset) which can result in consumers exploiting the differing views. A harmonised approach is required to remove tax distortions and to have a positive effect on tax revenue and the flow of goods and services across the globe. It will remove the risk of tax evasion and abuse of law[1].

There is an issue of enforcement of crypto currencies; how can a tax administration ensure that taxpayers are complying with their crypto currency-related reporting obligations? Most users of crypto currency will use a third party provider like Coinbase to manage their Bitcoin wallets. The U.S. for example could enforce U.S. crypto currency rules by pressuring Bitcoin service providers for information relating to any given transaction, however it is far more difficult if the intermediary were based in say, Bulgaria. Under the current treaty framework the IRS probably wouldn't be able to do anything about it. International co-operation is essential when you have a global payment method like Bitcoin to ensure Bitcoin taxation is enforced. Such a solution would be similar to the Foreign Account Tax Compliance Act (FATCA). Governments would target bitcoin exchanges instead of banks to get data on non-compliant taxpayers.

Tax Treatment for GST Purposes

To date, Bitcoin and other crypto currencies have been largely unregulated and have largely uncertain tax treatment. We know already that New Zealand regulates the currency market, why shouldn't the crypto currency market be regulated as well? The rise of crypto currencies has piqued the interest of international governments who are slowly realising that crypto currencies are here to stay as part of the constantly evolving digital currency. Globally regulators have struggled with the proposition of harnessing crypto currency but it has progressed and matured to the point where it requires legitimacy in order to encourage use but also to protect consumers. As crypto currencies increasingly acquire real economic value, they raise substantial issues.

One of the bigger issues that have been raised to date is how Bitcoin (and other crypto currencies) should be classified for the purposes of the Goods and Services Tax Act 1985 (GST Act). As you now know there has been conflicting regulation circulating the crypto currency, from the U.S treating Bitcoin as 'property' to Australia regarding Bitcoin as a 'taxable supply'. In determining whether crypto currencies are say, 'money', 'currency', 'services' or 'goods' for the purpose of the GST Act requires consideration of the characteristics of Bitcoin. If they are not treated as money, they would be similar to the way barter transactions work.

Importance of legal tender:

A long time ago people traded by barter. Money was invented because it solved many of the severe limitations of bartering enabling people to buy and sell to others far more easily. Money also allowed production and consumption to more easily happen at different times. It gives people the ability to save money and spend it later[44].

However for money to work it must have a reliable standard of value and to exchange goods and services for money you need to have confidence in money such as that money you receive will have roughly the same store of value when you wish to spend it at a later date. Legal tender helps provide this stability as it enables to government to regulate the currency market which in turn provides greater security when transacting in money.

Legal tender is a tender of payment that, by law, cannot be refused in settlement of a debt denominated in the same currency. The concept of legal tender is enacted by section 27 of the Reserve bank of New Zealand Act 1989 which gives an exclusive benefit to the currency issued by the Reserve Bank. However the Act does not specifically mention what 'legal tender' actually means and 'legal tender' is often commonly confused with the related concept of 'payment'. 'Payment' requires the consent of both the buyer and the seller. This is similar when offering to pay with legal tender. When offering to settle a debt in legal tender a valid tender has been made but this does not mean the payment is complete, the creditor must accept the payment. However the difference between 'payment' and 'legal tender' is that if the seller refuses to accept the tender they are barred from

[44] Reserve Bank of New Zealand. *Monetary Policy and Inflation.* Retrieved February 04, 2015, from http://www.rbnz.govt.nz/challenge/resources/2970552.html

recovering the debt in court. Therefore in practical terms, the creditor has little choice but to accept the legal tender payment or they have no way of recovering the debt[45].

Legal tender laws are designed to protect buyers however sellers can protect themselves from these laws in the following way if they wish to receive payment in something other than legal tender. Section 27 of the Act does not say that payment must be in legal tender or that payment in legal tender is sufficient for the debtor to meet their payment obligations, the actual form of payment is determined by the contractual context. If a creditor wishes to be paid in, say, potatoes, they must first specify this in the contract, which the debtor must accept.

In describing the legal characteristics of legal tender two fundamentally important ones are the right of the creditor to be paid in legal tender i.e. bank notes and coins that meet the statutory requirements of legal tender and the right of the buyer to offer legal tender as payment (unless stated otherwise in the contract). Legal tender guarantees a state's currency has an exclusive legal status and is good to settle debts.

The role of the government, reserve bank and banks

As I mentioned above it is possible to avoid the applicability of legal tender laws in trade via a contract however they are still important for helping the legal tender currency to circulate. Legal tender gives status to a government's currency, implicitly allowing them to reject any form of payment not in legal tender which creates a demand for legal tender, which makes it valuable. Taxpayers must obtain legal tender to pay their taxes. While a contract denominated in a foreign currency makes the legal tender laws irrelevant for your contract, receiving income in a foreign currency does not exempt you from paying taxes in *New Zealand dollars*. This means you must convert the foreign currency received to NZD. Thus taxpayers are willing to provide goods and services for legal tender[46].

The Reserve Bank of New Zealand Act 1989 confers power on the reserve Bank of New Zealand (RBNZ) to register banks and undertake supervision of those registered banks. A bank is not a regular business. It is carefully chartered and regulated by the government and generally has special privileges and obligations[47].The currency market is highly regulated by the government in order to encourage reliability, compliance, security, stability, certainty and confidence in legal tender.

Is Bitcoin 'money' for GST purposes?

Whether Bitcoin is 'money' is relevant for determining whether Bitcoin falls within the scope of 'goods and services' for GST purposes. The term 'goods' is defined in section 2 of the GST Act as including "all kinds of property and real property" but does not include 'money'. The term 'service' is defined as encompassing anything that is "not goods or money".

[45] McBride, N. Reserve Bank of New Zealand. *Payments and the Concept of Legal Tender.* Retrieved February 04, 2015, from http://www.rbnz.govt.nz/research_and_publications/reserve_bank_bulletin/2007/2007sep70_3mcbride.pdf

[46] Godlberg, D. Bar Ilan University. *Legal Tender.* Retrieved February 04, 2015, from http://www.biu.ac.il/soc/ec/wp/2009-04.pdf

[47] Ibid

Bitcoin treatment under current law

For the purposes of the definition of 'goods' and 'services' the relevant definition of money in section 2 is paragraph (a): "bank notes and other currency, being any negotiable instrument used or circulated, or intended for use or circulation, as currency". It must therefore be ascertained as to whether Bitcoin is a currency in order to determine whether it falls within the scope of 'goods and services'. Section 3(2) of the GST Act defines 'currency' as "any banknote or other currency of any country, other than when used as a collector's piece, investment article, item of numismatic interest, of otherwise than as a medium of exchange". Oxford Dictionary defines 'currency' as "the circulating medium; the money of a country in actual use". Both definitions define 'currency' as belonging to a specific country i.e. that 'currency' is regulated and backed by a particular government authority. Although Bitcoin is in *actual use* it cannot be said to be *of a country*. One of the key characteristics inherent in the Bitcoin protocol is that it is decentralised in that it has no central repository and no single administrator. Bitcoin is not backed by a government. New Zealand follows the OECD decision of treating products digitally supplied as services. This means that where the entire transaction occurs over the internet, like when bitcoins are debited form the miner's digital wallet and transferred to the purchaser's, the bitcoins remaining in their digitalised form are regarded as services. When bitcoins are transacted in their physical coin form i.e. like a Casascius coin, then this will constitute a supply of goods[48] when applying the current tax law to Bitcoin. In summary, this makes it clear that under current law regardless of whether Bitcoin treated as a good or a service they will fall within the scope of the GST Act and be liable to GST. This conclusion is in line with the Ruling issued by our Australian counterparts, the Australian Tax Office (ATO).

Why Bitcoin should be viewed as 'money'

An argument put forward by Emmett J in the Australian case *Travelex Limited v. Commissioner of Taxation (Travelex)* contends that "money is any generally accepted medium of exchange for goods and services and for the payment of debts. Currency and legal tender are examples of money. However, a thing can be money and can operate as a generally accepted medium and means of exchange without being legal tender. Money is that which passes freely from hand to hand throughout the community in final discharge of debts and full payment for commodities and without the intention of the person who receives it to consume it or apply it to any other use than in turn to tender it to others in discharge of debts or payment for commodities". The characteristics if Bitcoin substantially fit this interpretation of money. The difference between Bitcoin and other non-cash payment system, like frequent flyer miles, is that bitcoins are accepted equally without reference to the character or credit of the person who offers it, or the legal relationship between the parties to the transaction[49], thus Bitcoin is more like money than these other types of payment systems. Bitcoin satisfies the functional aspect of money because it serves as a medium of exchange, a unit of account and a store of value. The crypto currency also shares the characteristic of 'negotiability' with cash[50]. When a bitcoins are transferred, ownership of the bitcoin transfers completely. It has an increasing acceptance within the community as a means of discharging debts and acquiring goods and services, it could be argued that it has reached a point where it now qualifies as money.

Despite this, custom alone cannot make something money in the absence of an exercise of monetary sovereignty by the State. For something to be money in a modern sense it must exist within some legal framework because it reflects an exercise of sovereignty by the State in question and enables

[48] Jamison, S.. *Bitcoin*. Inland Revenue.
[49] Bitcoin Association of Australia. Position Paper.
[50] Ibid

proper regulation of money transactions. It could be suggested that new law be put in place that enables the classification of Bitcoin as 'money' but not legal tender.

In the present day, Bitcoin wealth is arbitrarily concentrated in the hands of its early adopters. Currency ultimately derives its value from the willingness of other people to provide goods and services in exchange for that currency. While there will always be a niche of people (techies most likely) willing to exchange things for bitcoin, it is unclear why the majority of New Zealanders would be willing. Bitcoin is volatile and more confusing and harder to grasp in concept than fiat currency which is more secure, stable and easier to trade in, thus it is dubious as to whether Bitcoin could ever be eventually considered a currency legally equal to fiat. However at first mobile phones were difficult to operate, not used by many and overtime the everyday man has evolved to understand the technology and many now use a mobile device in everyday life. Bitcoins are capable of being generally accepted and can be accepted electronically by anybody with a Bitcoin wallet.

Outside scope