Privacy Commissioner
Te Mana Matapono Matatapu

International Disclosures

and

Overseas Information and Communication Technologies Survey

May 2011

Contents

Introduction

Understanding cloud computing is increasingly becoming a priority for business and government alike. How can we take advantage of the benefits that the various types of cloud services can offer, while still preserving security and privacy of information, and the trust of the people we serve?

The Office of the Privacy Commissioner is frequently asked for advice and guidance on identifying and managing risks with cloud services. However, it is difficult to develop guidance unless we understand how agencies are thinking about and using overseas-based information and communication technologies (ICT). There has been little empirical work in New Zealand that helps us to see what is currently going on.

This is why we have done this survey. We asked a broad range of public and private sector agencies to tell us about their experience with international disclosures and overseas-based ICT infrastructure. This has given us a useful perspective on what is happening on the ground.

We deliberately avoided asking questions that referred to “the cloud”. Cloud computing can mean different things to different people, and we wanted to avoid any potential for confusion. Instead, we identified four separate ways in which personal information might end up overseas (see the Methodology section).

New Zealanders’ information increasingly does not stay in New Zealand. We are a member of the global community. As individuals, we send our own information offshore all the time – for example when we buy goods, use smartphones or participate in social media. Government and businesses also act internationally as well as locally.

So it was not a surprise that our survey showed a strong tendency to disclose personal information to offshore agencies. What we were particularly interested in was how those disclosures are made and what controls exist to protect the privacy and security of that information.

Slightly more than half of the 50 respondents disclose personal information to overseas organisations for those organisations’ own use. About half of the agencies make disclosures on a regular basis.

Notification to individuals about what was happening with their information was mixed. Some form of notification was reasonably common for disclosures to overseas organisations for those organisations' own use, but became more uncommon as the survey progressed. This indicates that individuals frequently will have no idea that their information is being stored or processed overseas.

Just over a third of the 50 agencies surveyed use overseas-based infrastructure for processing or storing personal information, or similar.

Decisions to use overseas infrastructure were predominantly made on an ad hoc basis. Relatively few agencies had policies to help them make those decisions.

A vast majority of agencies used mobile internet or email devices such as smart phones. However, most of those agencies said that they did not use overseas infrastructure. Obviously, therefore, many agencies did not perceive use of these devices as involving overseas infrastructure.

As a result, we now have a clearer picture of how agencies can better understand and mitigate ICT risks, and develop good privacy practice that will enable them to get the most out of cloud services. There is still a lot of ground to cover in this rapidly developing field. However, we hope that this survey provides a useful platform for future discussions.

Methodology

This is the first time the Office of the Privacy Commissioner has undertaken a survey on sending information offshore and using offshore ICT. We designed the survey specifically to collect the kind of information we will need to develop useful guidance for the public and private sector.

We decided not to directly refer to “cloud computing” in our survey. This is because there is confusion about what cloud computing is. There are many different definitions because it is still an emerging field. Instead, we chose to focus on overseas-based ICT infrastructure, which is a concept most people are familiar with. The concept shares many privacy issues with cloud computing, and so the survey questions will give us clear information to work with.

Who we asked

We are interested in the practices and experiences of both public and private sector agencies, so we approached both. The survey was optional, so we approached as many suitable agencies as was practical to obtain a reasonable sample size. The list of agencies that responded to the survey is set out below.

We contacted the same public sector agencies that participated in our Portable Storage Device (PSD) survey last year. We approached 35 public sector agencies and received 33 responses.

The private sector list was compiled using a mix of our current contacts and agencies on the NZX 50 that we believed may handle a significant amount of personal information. We approached 44 private sector agencies and received 17 responses.

We wrote directly to the Chief Executive (or similar) of each identified agency requesting their assistance. We also sent an electronic version of the survey to each agency's Chief Information Officer or Privacy Officer to complete.

Just days after the survey had been distributed, the February earthquake in Canterbury struck. Understandably, a number of the agencies we had approached could not respond to the survey within the original timeframe. The deadline was extended by two weeks to allow agencies additional time to respond if they wished.

Participating Agencies

Private Sector

AA Insurance Ltd
Air New Zealand
ANZ National Bank
ASB Bank Limited
AXA New Zealand
Bank of New Zealand
Designer Technology Limited
Fonterra
GE Finance and Insurance
Harbour Health PHO
Meridian Energy Ltd
New Zealand Post
Nurse Maude Association
ProCare Health Limited
Television New Zealand Limited
Tower Insurance
TSB Bank

Public Sector

ACC
Crown Law Office
Department of Building and Housing
Department of Corrections
Department of Labour
Department of Internal Affairs
Department of Prime Minister and Cabinet
Government Communications and Security Bureau
Inland Revenue Department
Land Information New Zealand
Ministry of Economic Development
Ministry for the Environment
Ministry of Agriculture and Forestry
Ministry of Culture and Heritage
Ministry of Defence
Ministry of Education
Ministry of Fisheries
Ministry of Foreign Affairs and Trade
Ministry of Health
Ministry of Justice
Ministry of Pacific Island Affairs
Ministry of Science and Innovation
Ministry of Social Development
Ministry of Transport
Ministry of Women's Affairs
New Zealand Customs Service
New Zealand Police
New Zealand Security and Intelligence Services
Serious Fraud Office
State Services Commission
Statistics New Zealand
Te Puni Kokiri
Treasury

What we asked

The survey itself is attached as an appendix. It was made up of two main parts. Section A addressed the disclosure of information to overseas organisations. Sections B to D addressed the use of overseas-based ICT infrastructure. The following outline expands a little more on the types of questions that were covered.

Section A: International Disclosures

This section focused on whether and how agencies send personal information from their agency to any organisation overseas – not for the purposes of storage or processing, but for that organisation's own use.

Section B: Overseas Information and Communications Technology (ICT)

This section was an introduction to the following sections (C&D). It asked general questions about the use of ICT infrastructure overseas and how agencies make decisions to use it.

Section C: Overseas ICT owned and managed by your organisation

This section was about how agencies use computing infrastructure that they own but which is based overseas, for example, an international branch/head office of an organisation.

Section D: Overseas ICT owned and managed by a third party

This section covers what is sometimes called "the cloud". We asked how agencies use overseas third party-owned ICT infrastructure, for example, to store or process information.

Summary of results

New Zealanders' information increasingly does not stay in New Zealand. We are a member of the global community and our Government and businesses also act internationally as well as locally.

Our survey showed a strong tendency to disclose personal information to overseas organisations. We were particularly interested in how those disclosures are made and what controls exist to protect the privacy and security of that information.

Disclosures to overseas organisations for their own use

How often do disclosures happen and where does the information go?

- Slightly more than half of the 50 respondents disclose personal information to overseas organisations for those organisations' own use.
- Most of these disclosures (74%) involve only small amounts of personal information at a time. About half of all these disclosures are on a regular basis.
- Those organisations are mostly in Australia, but information is also sent to other Asia-Pacific countries as well as to the United States, Canada and the European Union.
- Public sector agencies tend to disclose information to overseas public sector organisations.

What authority is there for those disclosures?

- While it is common for legislation to authorise those disclosures, individuals also often give express permission for the disclosure

What controls are there over misuse of the information once it is overseas?

- Most agencies have controls to protect the security of the information in transit, but some do not.
- Most agencies place controls on the information so overseas organisations cannot pass it onto unauthorised third parties or use it for different purposes.

- However, some agencies reported that they either had no control over what happened once the information was sent overseas, or did not know whether they had control.

- Although most agencies said they had control over misuse of information, a smaller number than expected took active steps to check how the overseas organisations were using and managing the information they had sent.

The use of overseas infrastructure

How often do New Zealand agencies use overseas infrastructure?

- A majority of agencies said they do not use overseas ICT infrastructure for their business functions. Most of those agencies had no need to use overseas infrastructure or did not see a benefit in it. However, a relatively significant number (10) were influenced by privacy concerns.

- Just over a third of the 50 agencies surveyed use overseas ICT infrastructure for processing or storing personal information, or similar. Of those agencies, over half were private sector agencies – 10 of the 33 public sector agencies use overseas-based ICT infrastructure compared with 11 of the 17 private sector agencies.

- 14 agencies indicated that they use infrastructure that is overseas but owned by the agency

- 18 agencies indicated that they use overseas infrastructure owned and managed by a third party provider – that is, ‘cloud’-style ICT.

Where is the overseas infrastructure that agencies use?

- For those agencies using overseas infrastructure they own, that infrastructure was mostly based in Australia, although several agencies used facilities in the United States and the European Union, or Asia-Pacific countries.

- The third-party providers of cloud-style ICT were usually based in the United States or Australia. The infrastructure itself (eg servers) was also most commonly located in the United States or Australia, though there was a wide range of countries involved, for example in Asia.

What controls are there over the information on the overseas infrastructure?

- The 14 agencies that use overseas infrastructure that they themselves own had strong controls over access (access restricted by role) and security (encryption and routine checks).
- Security was obviously a major consideration for the agencies sending information to third party providers – encryption, for instance, was common.
- However, other forms of control were less convincing. A small number of agencies said they had no control (even through contractual conditions) over whether the third party provider could use the information for its own purposes or pass on the personal information to others without authorisation. And a larger number did not check how the provider used or managed the information.
- Two agencies were not convinced that information could be retrieved easily if the individual asked for access to it.
- Retention also raised some concerns. While half the 18 respondents said that the third party provider only kept the information for as long as the respondent agency needed it (and a few providers kept a backup for a short time), three agencies had no idea how long the information was retained and two said that the provider kept the information indefinitely.

Who are the major third party providers of ICT?

- Our survey indicated that there is no clear leader in the market. The agencies used a very wide range of providers.

How are decisions made about whether to use overseas ICT?

- 15 agencies said they used internal policies to decide when to disclose personal information to overseas organisations for those organisations' own use. However, 14 agencies make those decisions on a case-by-case basis.
- Decisions to use overseas infrastructure were predominantly made on an ad hoc basis. Relatively few agencies had policies to help them make those decisions.
- There therefore seems to be a gap. Even those agencies that already use overseas infrastructure do not always have a structured way of deciding how or whether to do that.

Are individuals told when their information is sent overseas?

- For disclosures to overseas organisations for those organisations' own use, notification to individuals about what was happening with their information was mixed. Some form of notification was reasonably common – even if that notification was not direct, but was included in the terms and conditions or on the agency's website. However, 13 agencies indicated that they do not tell the individual at all, and 7 said that they only tell the individual if that person asks.
- Notification became more uncommon as the survey progressed.
- The majority of the 13 agencies who used their own overseas-based infrastructure did not notify individuals that their information was being stored overseas, or only told the individuals if they asked. Only three told the individual when the information was collected or had a notice in their terms and conditions.
- The same was true of the agencies that used third party overseas ICT. The majority either did not tell the individual or only told them if they asked. Some had a notice in the terms and conditions or on the agency's website, and a small number (3) told the individual at the time of collection.
- This indicates that individuals frequently will have no idea that their information is being stored or processed overseas.

The use of smart phones

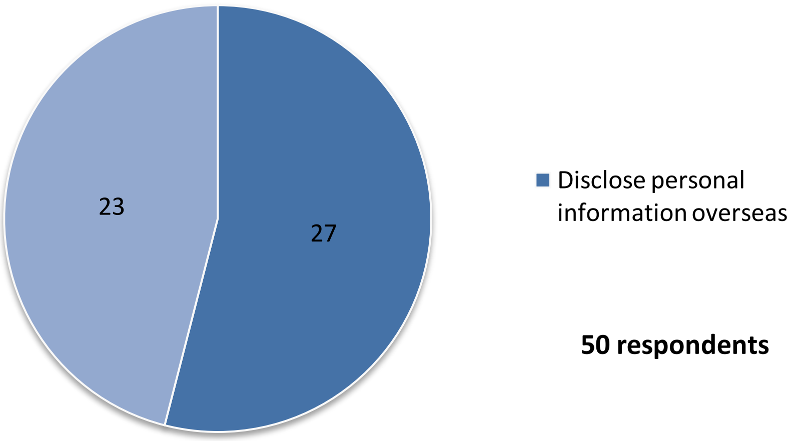
- A vast majority of agencies used mobile internet or email devices such as smart phones. However, most of those agencies said that they did not use overseas infrastructure.
- Obviously, therefore, many agencies did not perceive use of these devices as involving overseas infrastructure.

Results

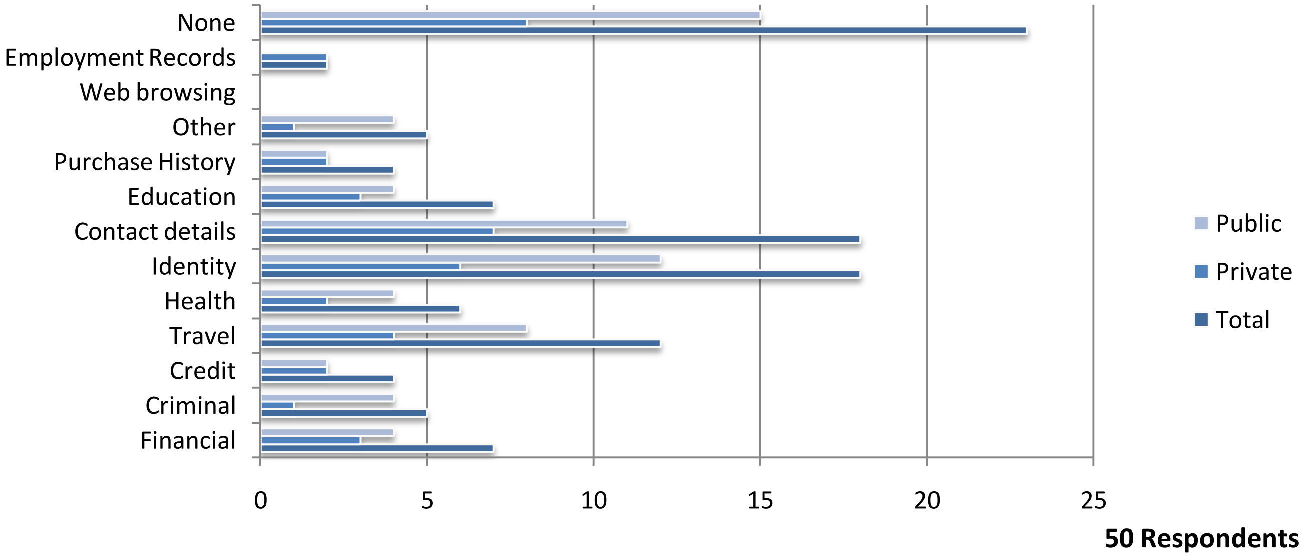
Section A

This section focused on whether and how agencies send personal information from their organisation to any organisation overseas – not for the purposes of storage or processing, but for that organisation's own use.

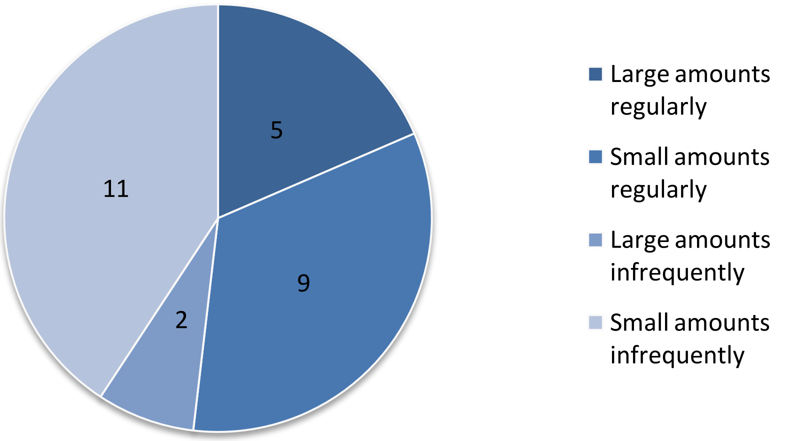
A1 Does your organisation disclose any of the following types of personal information to overseas organisations?



In terms of the split between public and private, roughly half of both the public sector agencies and the private sector agencies answered that they disclose information to overseas organisations.



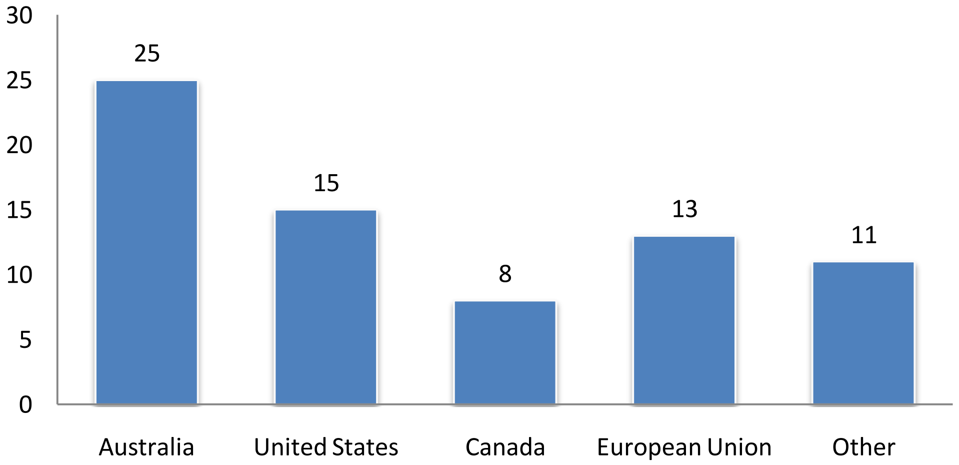
A2 How much personal information does your organisation disclose to overseas organisations?



27 Respondents

Out of the 27 agencies that share information with overseas organisations, there was a relatively even split between those that disclose information on a regular basis, and those that do so infrequently. In addition, the bulk of information transfers undertaken were for small amounts, rather than batch transfers.

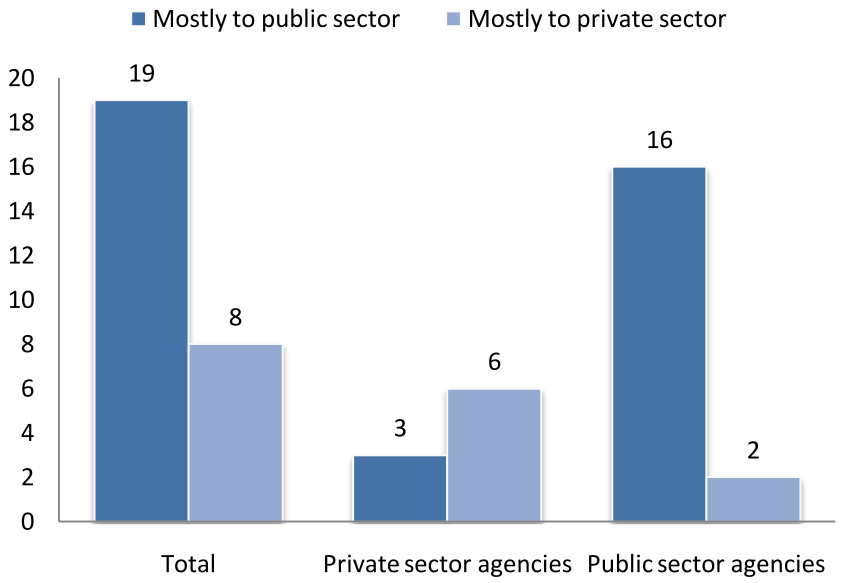
A3 Where are the overseas organisations to which you disclose personal information?



27 Respondents

Countries listed in the “other” field included China, Hong Kong, Japan and other parts of Asia as well as the Pacific Islands.

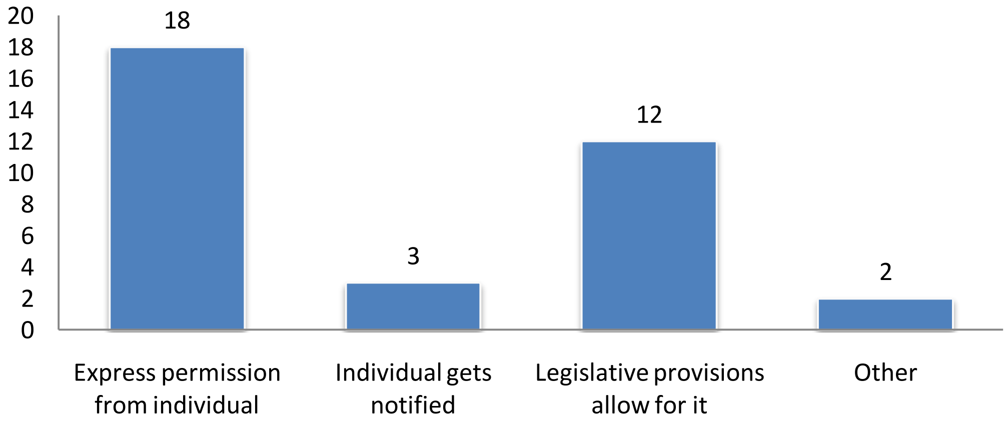
A4 Are those overseas organisations mostly public sector or private sector?



27 Respondents

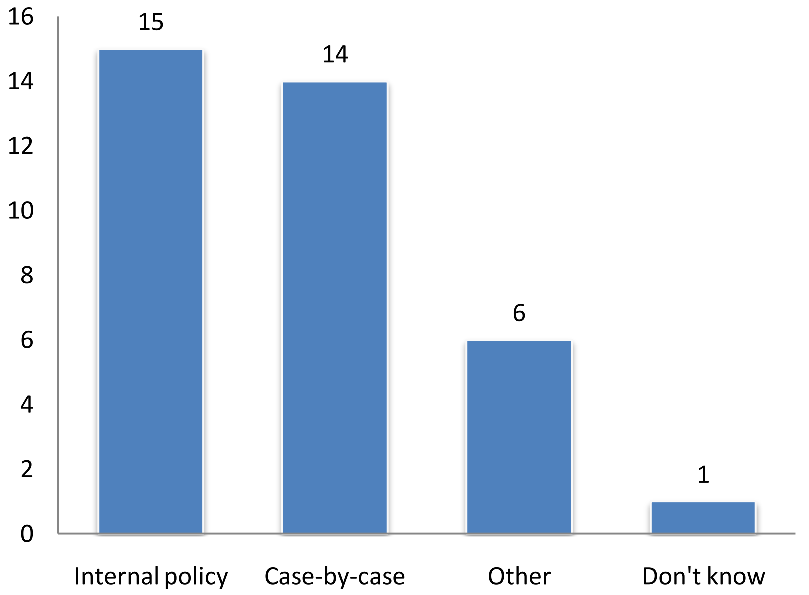
While there were too few private sector responses to draw specific conclusions, public sector agencies for the most part disclosed to overseas public sector agencies. Overall, 8 agencies (6 private, 2 public) disclose mainly to private sector agencies, while 19 agencies (3 private, 16 public) disclose mainly to public sector agencies.

A5 How is the personal information disclosure authorised?



27 Respondents

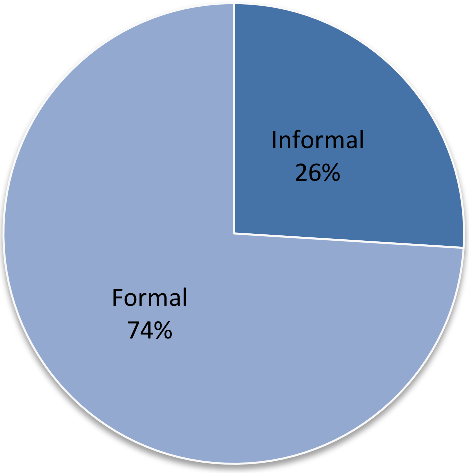
A6 How does your organisation decide when to disclose personal information to overseas organisations?



27 Respondents

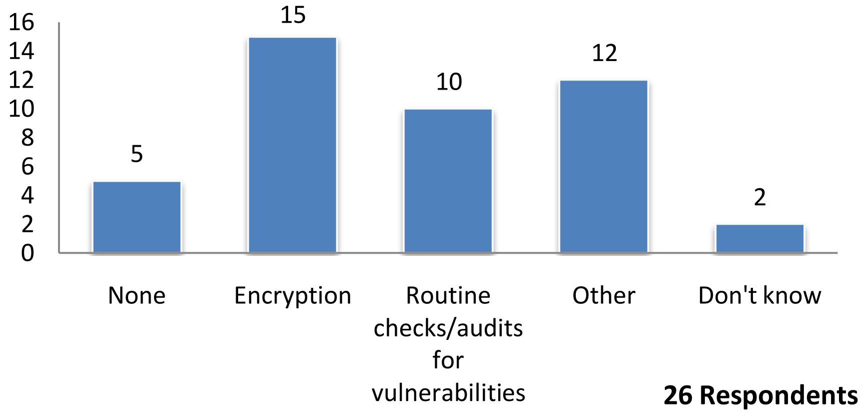
A7 How is this relationship managed with the overseas organisation?

In response to this question, a quarter of respondents selected “Contract”, just under a quarter selected “MOU” – over half of the responses were “Other”. The following graph categorises all responses as either formal (including Contract and MOU) or informal.



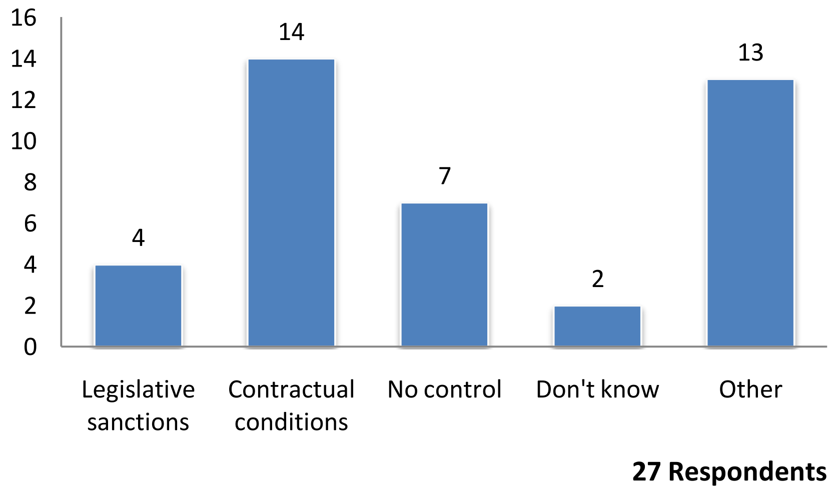
27 Respondents

A8 What controls are in place to ensure security of personal information as it travels between here and the overseas organisation?



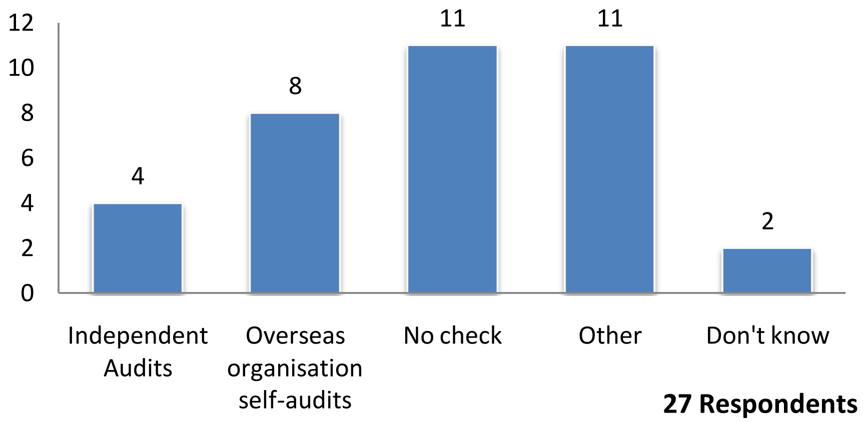
Various methods were listed under "other", ranging from diplomatic bag or secure servers to receipt acknowledgments and confidentiality agreements.

A9 How does your organisation control whether the overseas organisation can then pass the personal information onto unauthorised third party organisations or use it for purposes other than those it was originally collected for?



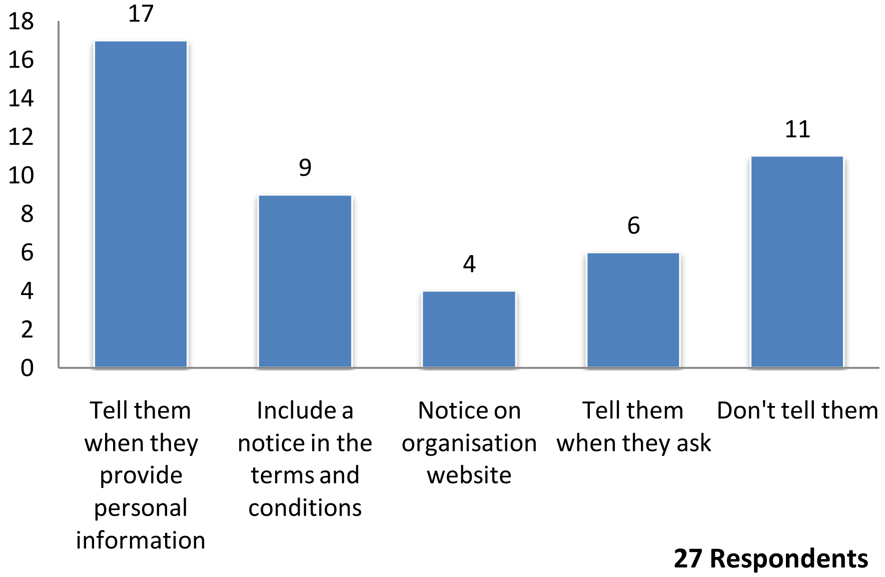
The "other" field gave a range of formal and informal arrangements, such as including conditions of use with each release, seeking assurance that use is limited, only sharing with trusted sources and having privacy agreements in place.

A10 How do you check the overseas organisation's use and management of your information?



Many of the entries under "other" served to give further information on the audits used, but also included measures such as including "seed" records or verifying that the overseas organisation has government accreditation.

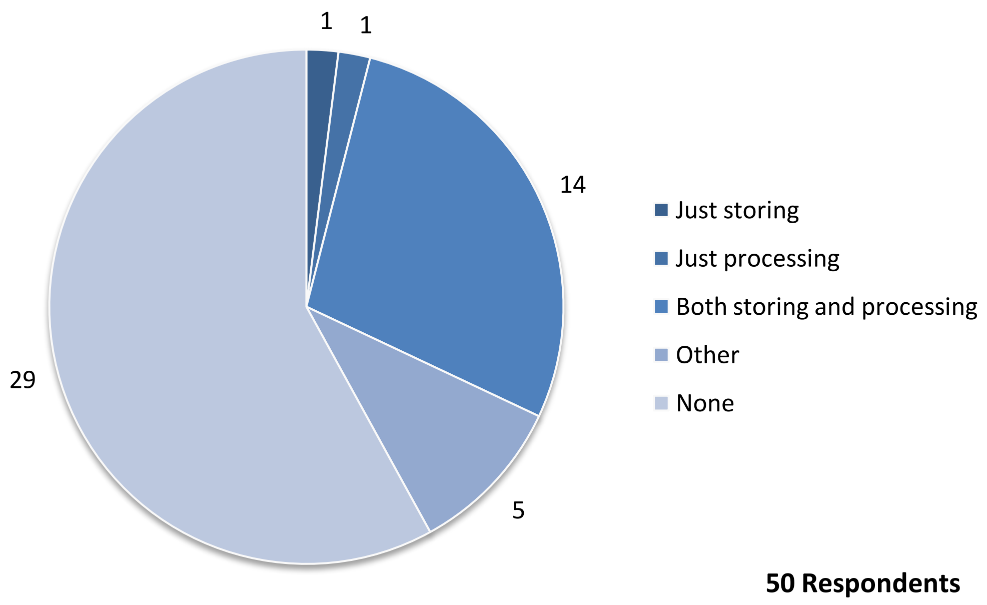
A11 How does your organisation tell the individuals concerned that their personal information is shared with an overseas organisation?



Section B

This section was an introduction to the following sections (C&D). It asked general questions about the use of ICT infrastructure overseas and how agencies make decisions to use it.

B1 Does your organisation use overseas infrastructure for any of the following?

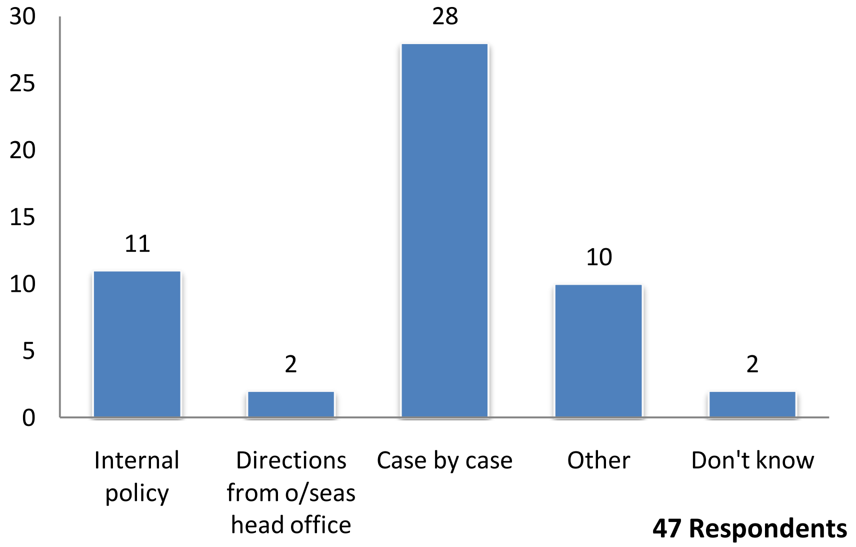


Just over a third of the 50 agencies surveyed use overseas-based infrastructure for processing or storing personal information, or similar. Of those agencies, over half were private sector agencies – 10 of the 33 public sector agencies use overseas-based ICT infrastructure compared with 11 of the 17 private sector agencies.

B2 If you answered "None of the above" to B1, why?

From the 29 agencies that answered this question, the main reason selected for not using overseas-based ICT infrastructure was that there was no need or benefit. Privacy concerns were also of note; ten agencies selected this option.

B3 How does your organisation decide when to use overseas ICT infrastructure?

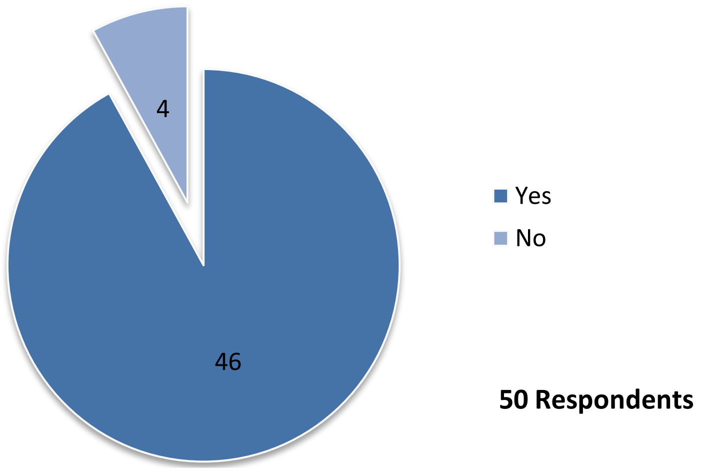


B3a If you answered "Internal policy/rules" to the above, do those policies or rules cover any of the following?

We asked if agencies' policies covered: the use of personal information by an overseas organisation; onward disclosure to a third party by an overseas organisation; specific guidance for handling personal information; and/or recognition of New Zealand's privacy laws.

Of the eleven agencies that answered this question, all indicated that their policies consider New Zealand privacy laws. Seven of these eleven agencies had specific guidance on the handling of personal information. Three addressed the use of information by an overseas organisation and three addressed onward disclosure by an overseas organisation.

B4 Does your organisation use mobile internet/email devices, such as smartphones?



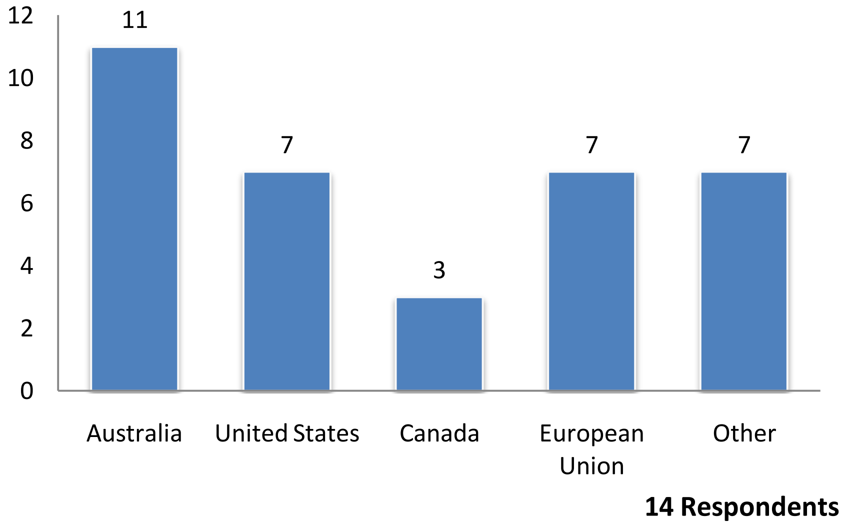
B5 Whose overseas infrastructure does your organisation use?

Your own organisation's (e.g. international branch of your organisation)	**6**
A third party's	**11**
Both	**7**
Don't use overseas infrastructure	**26**

Section C

This section was about how agencies use computing infrastructure that they own, but which is based overseas – e.g. an international branch/head office of an organisation. Fourteen agencies answered this section.

C1 Where is the overseas infrastructure located?



Under "Other" the following countries and regions were listed: Japan, China, the Pacific Islands, Singapore, other parts of Asia and the Middle East.

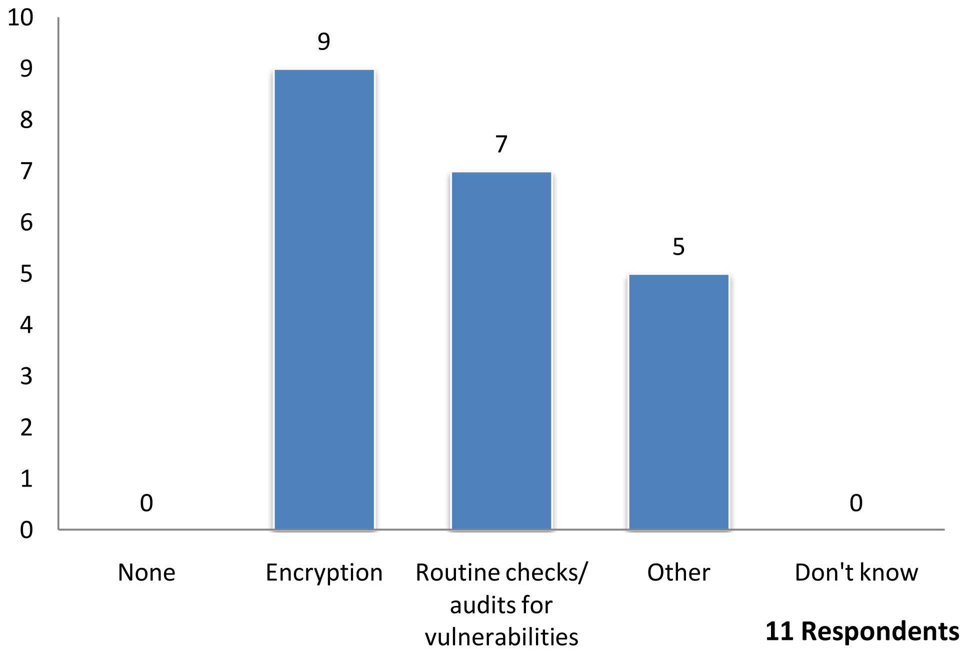
C2 Who can access the personal information stored on the overseas infrastructure?

All those that answered this question have role-restrictions in place on who can access the information. Twelve allowed a mixture of New Zealand and overseas staff access, while one restricted access to only New Zealand staff.

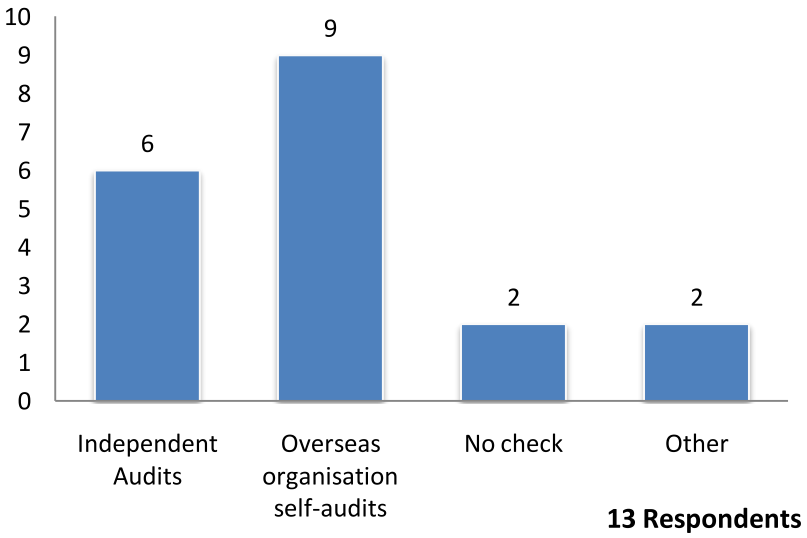
C3 If a client in New Zealand requests access to their personal information, can it be retrieved easily?

All thirteen respondents to this question answered yes.

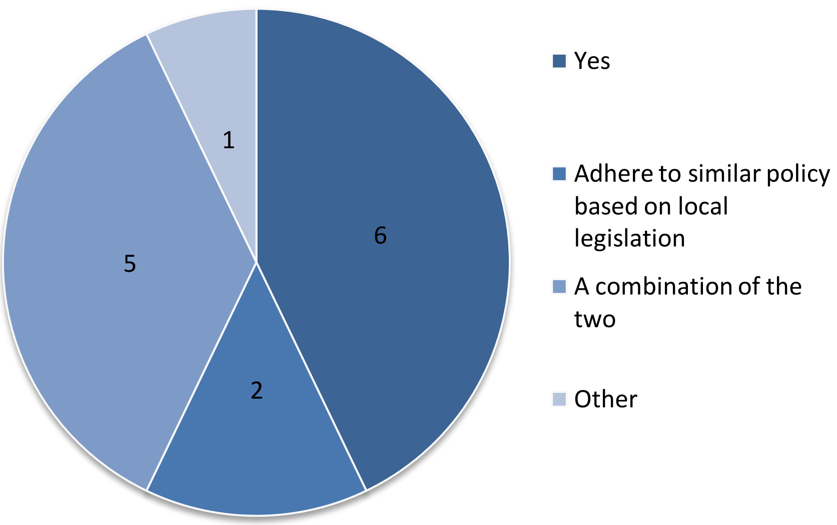
C4 What controls are in place to ensure security of personal information as it travels between here and the overseas location?



C5 How do you check the use and management of your information overseas?

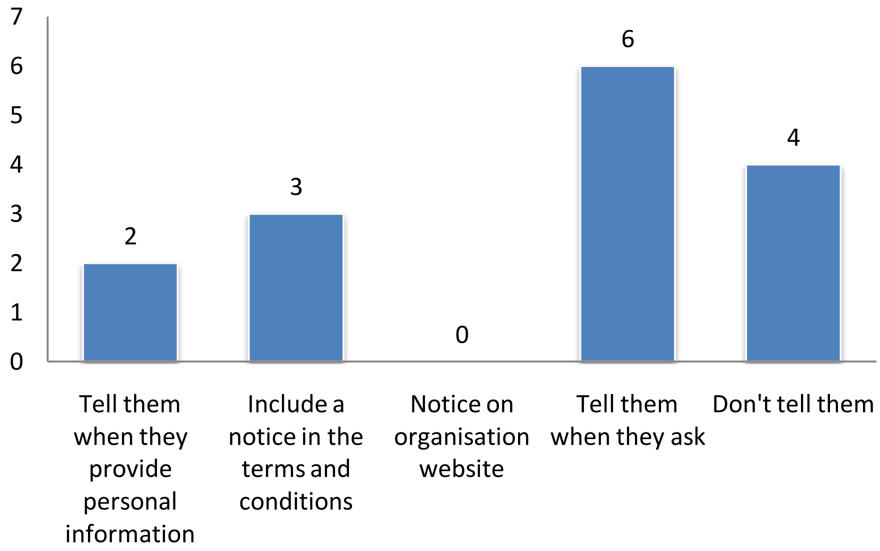


C6 Does the part of your organisation running the ICT infrastructure overseas operate under the same privacy policy as the part based in New Zealand?



13 Respondents

C7 How does your organisation tell the individuals concerned that their personal information is stored overseas? [Select all that apply]

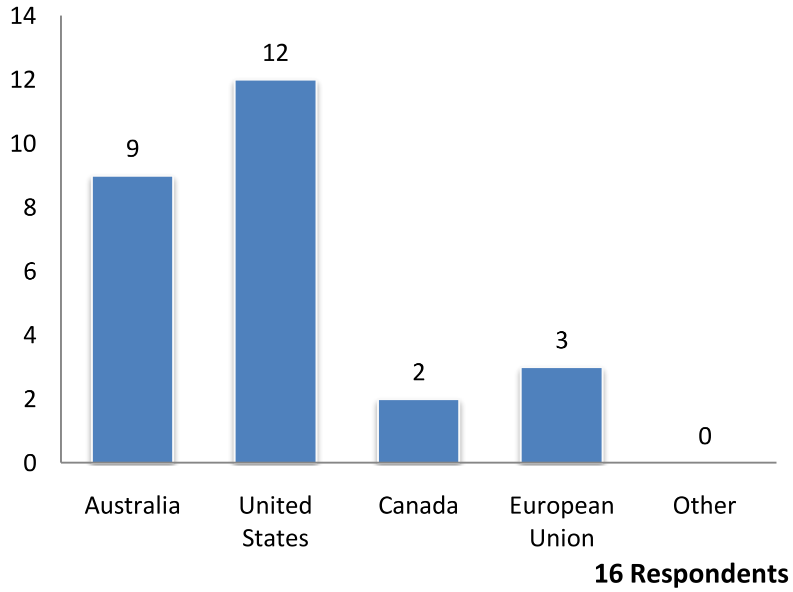


13 Respondents

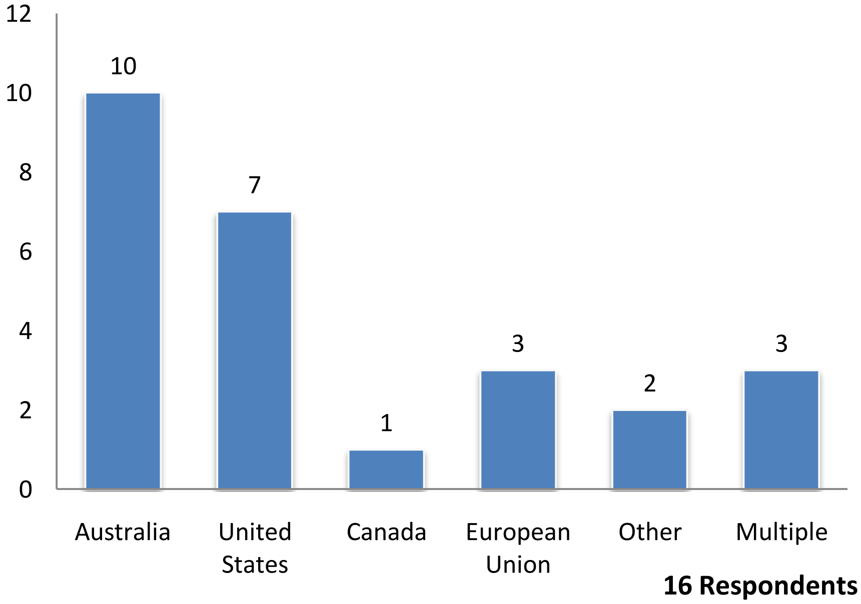
Section D

This section covers what is sometimes called “the cloud”. Because definitions of “the cloud” vary, we chose to focus specifically on asking how agencies use overseas third party-owned ICT infrastructure, for example to store or process information.

D1 If you use an overseas third party ICT solution provider (third party provider) where is their head office based?



D2 Where is the infrastructure that they use based?

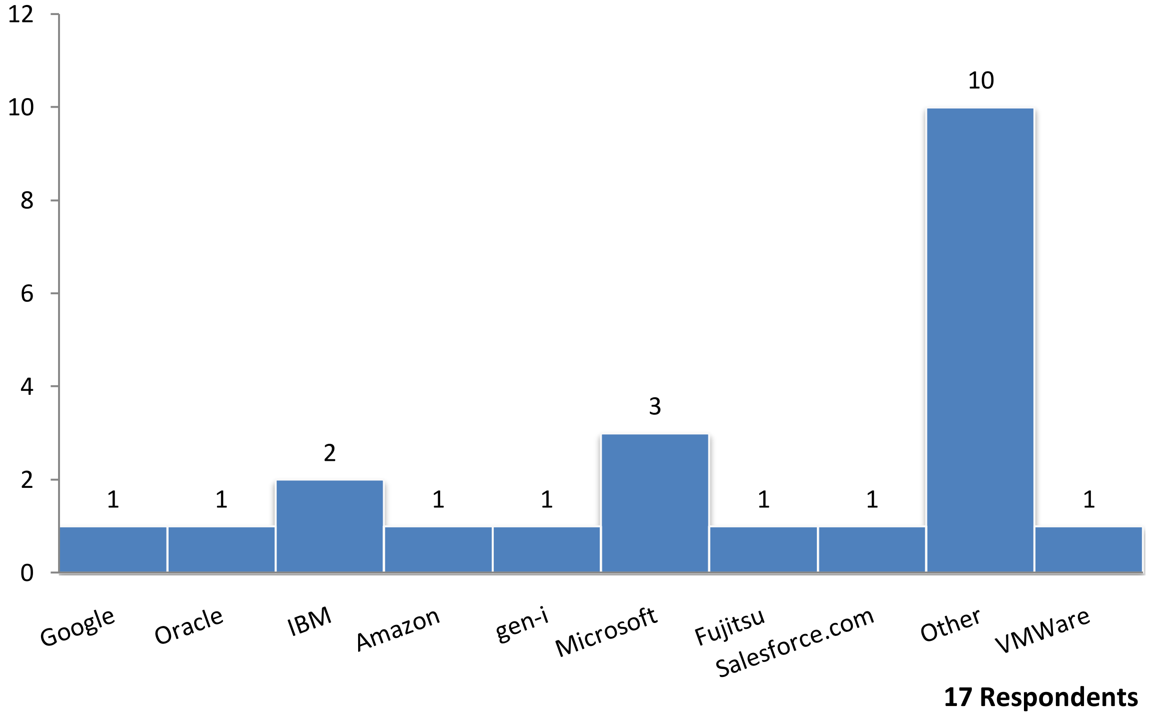


Singapore and India were listed under "Other".

D2a **Can your organisation choose the country that the third party provider uses for the storage or processing of your information?**

Of the three agencies who answered this question, two agencies answered no, and one yes.

D3 **Which of the following providers does your organisation use for your overseas ICT solutions:**

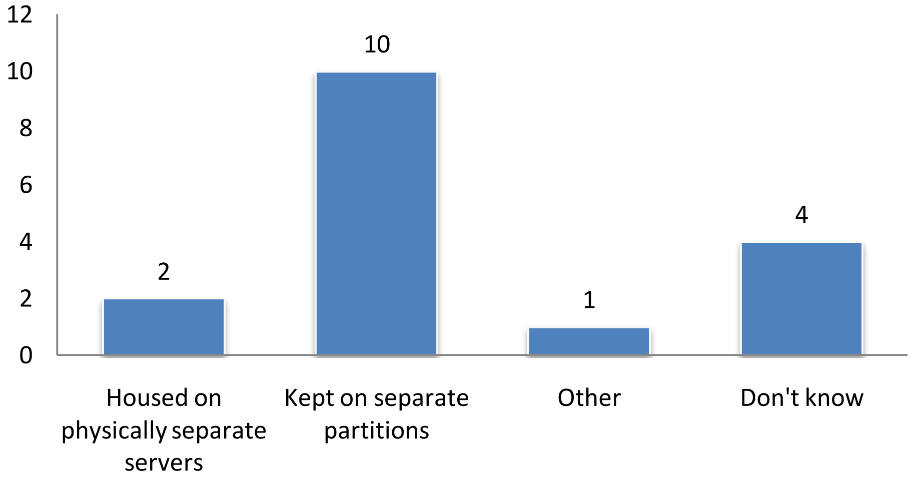


Within the "Other" category, responses did not indicate any dominant provider. There was very little repetition among the providers listed in this field.

D4 **Who can access the personal information?**

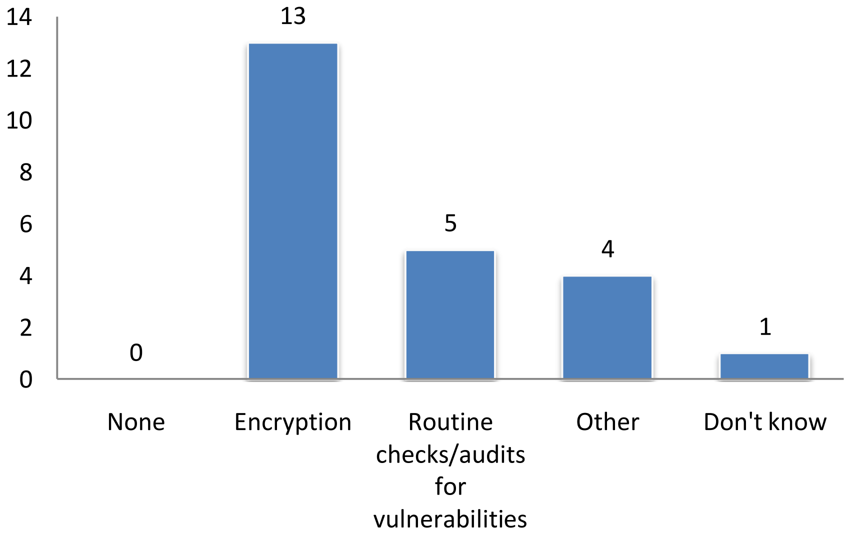
Thirteen respondents indicated that there were role restrictions in place for either New Zealand staff or the third party's staff – six of these not allowing the third party's staff access to the information at all. The remaining four agencies also did not allow the third party to access the information, but did not place role restrictions on the ability of New Zealand staff to access the information.

D5 **How is the personal information from your organisation kept separate from other organisations' data housed in the third party provider's infrastructure?**



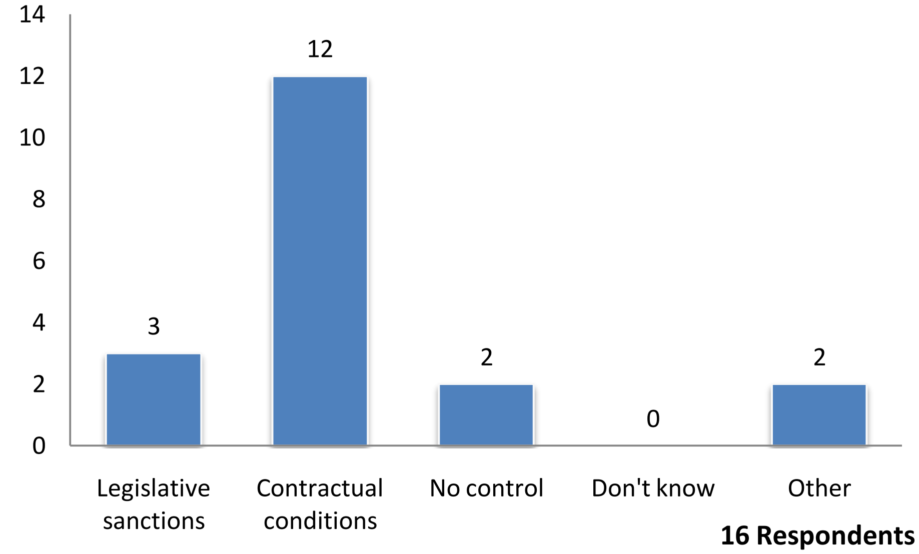
17 Respondents

D6 **What controls are in place to ensure security of personal information as it travels between here and the overseas location?**

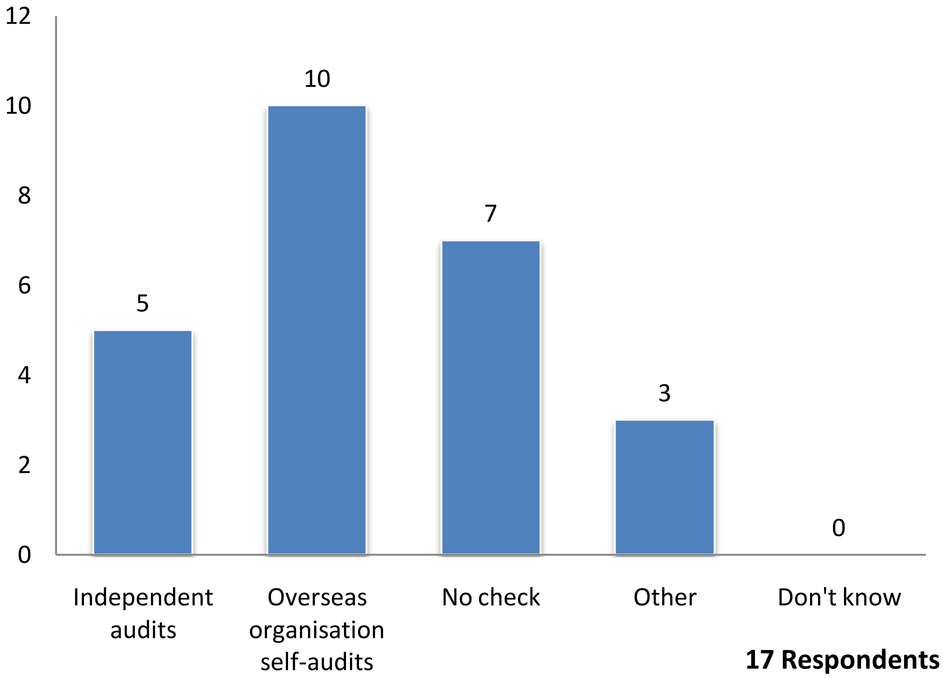


15 Respondents

D7 How does your organisation control whether the third party provider can use your organisation’s information for its own purposes, or pass on the personal information to unauthorised third parties?



D8 How do you check the third party provider’s use and management of your information?

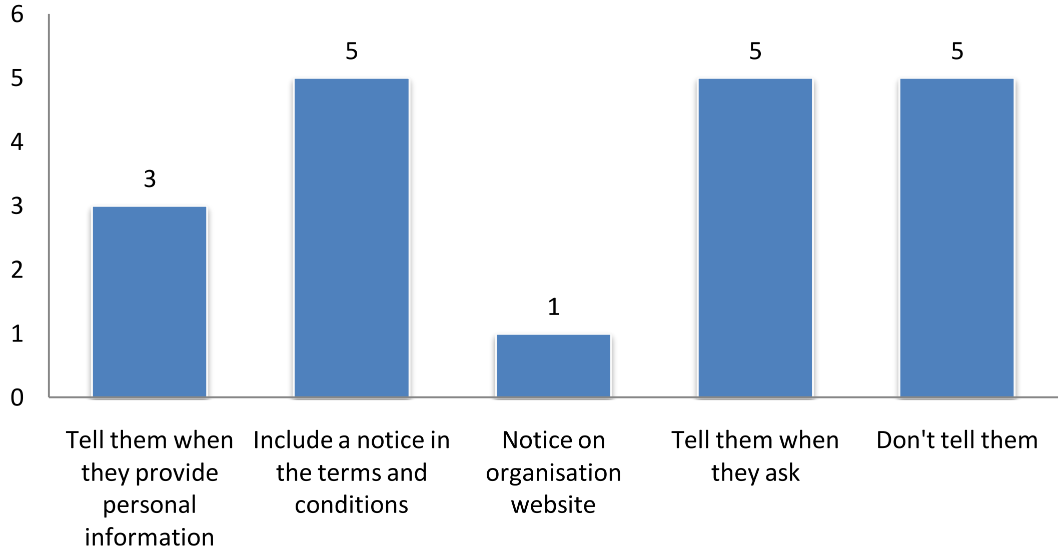


Under "Other", measures such as checking a supplier's track record were given.

D9 **If a client in New Zealand requests access to their personal information, can it be retrieved easily?**

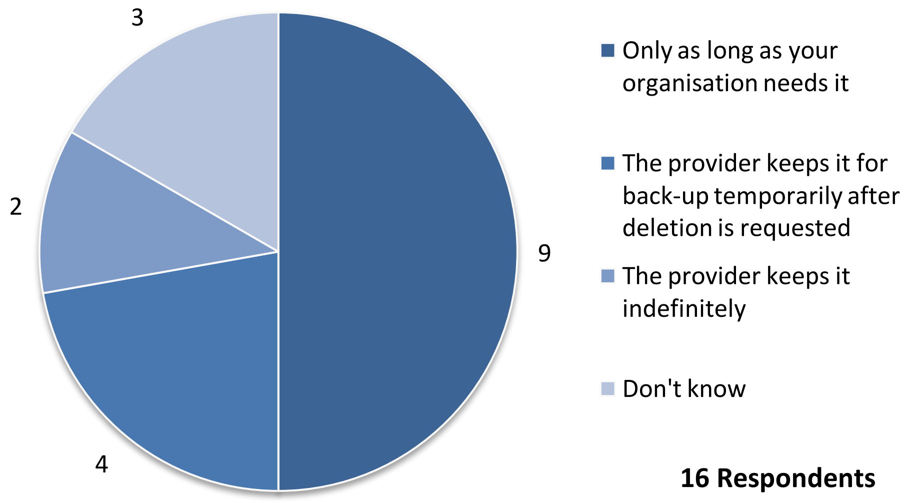
Fifteen of the seventeen organisations who answered this question answered ‘yes’. One said no, and one did not know.

D10 **How does your organisation tell the individuals concerned that their personal information is stored with an overseas third party provider?**



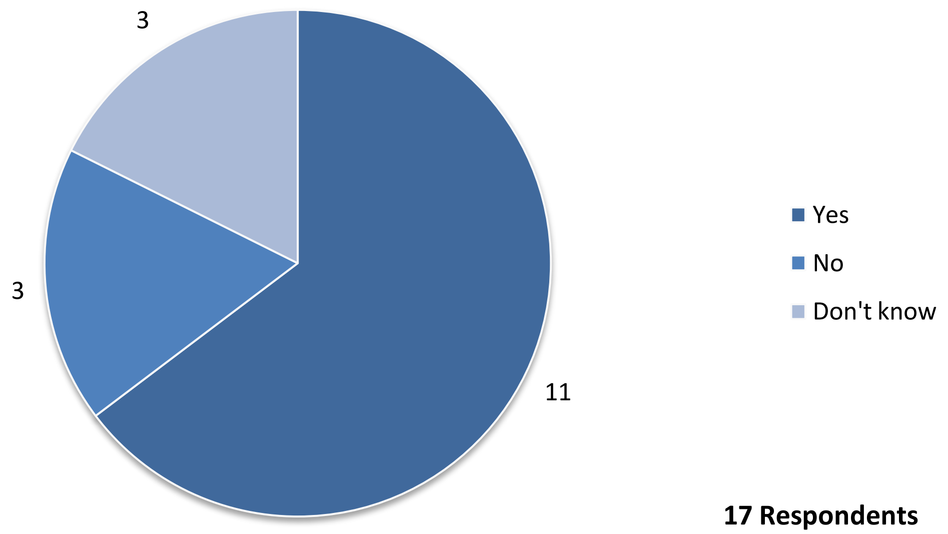
16 Respondents

D11 **How long does the third party provider hold the personal information for?**



16 Respondents

D12 Is there provision for the third party provider to dispose of or destroy your data on termination of their contract with your organisation?


Yes
No
Don't know
17 Respondents