trademe
Group Limited

Transparency Report 2017

Contents

Introduction

Our members place a lot of trust in us to protect their personal information, and keeping their information safe is a priority.

Our members' personal information has continued to be of interest to government agencies over the last 12 months.

As a responsible company we sometimes need to release information to third parties, and we are upfront about how and when we share data because we value our members' trust.

Our fifth annual Transparency Report details the requests we've received, and our responses, over the last 12 months (1 July 2016 through to 30 June 2017).

We've also taken the opportunity to set out our thoughts on several privacy-related issues, and what we think about them. Being 'honest and straight up' is enshrined in our company values, and we think this report helps our community understand our approach to privacy.

Releasing information – when we have to and when we choose to

In last year's report, we discussed the fine line between information releases where we're *compelled* under law to release information, and where we *choose* to release it under the Privacy Act.

A compulsory release might occur when the Ministry of Social Development is investigating benefit fraud, and compels us to share everything we have on a member under its statutory powers. In this case, we must comply.

On the other hand, when the Accident Compensation Corporation investigates the same kind of behaviour, they have no such powers and therefore need to request that we voluntarily release information under principle 11(e) of the Privacy Act (the "law enforcement" exception).

In the latter case, we make the call to release information if the requesting agency satisfies us that the exception applies. This is our call to make. Agencies have no powers to force us to release information under the Privacy Act.

We regularly reject requests for voluntary disclosure if we're not satisfied the requirements in the Privacy Act have been met. We call this 'pushing back'. We may ask the agency to refine their request so it's more targeted or relevant, or reject the request altogether.

It's also common to receive legitimate requests (i.e. where the Privacy Act permits disclosure), where we do not release any information in response to that request. This differs from a push–back and could be in circumstances where no information exists, or the information Trade Me holds falls outside the scope of the request.

Based on the total number of requests we received in the reporting period, we released information for 13% of enquiries pursuant to a compulsion order, 62% under the Privacy Act, and nothing was released in relation to the remaining 25%.

We've broken it down into requests from the New Zealand Police and government agencies below.

This is a call for more transparency reporting in New Zealand

As far as we can tell, we're still the only New Zealand-based company regularly publishing a transparency report. This is despite encouragement and assistance offered by Internet NZ to other businesses, and the results of a **transparency reporting trial** run in 2016 by the Office of the Privacy Commissioner (OPC).

We get approached relatively regularly by businesses interested in taking the plunge and getting into transparency reporting. Based on this interest, we're surprised more businesses aren't following through and starting to report.

Admittedly, it's a big decision for businesses to make, especially if they have concerns their users will not support the choices they're making around data releases to government agencies. We had the same concern before we published our first report but having opened up about what we do, we've never looked back.

We think there are solid benefits to transparency reporting. We firmly believe that telling our members how their data is used actually gives them confidence we're doing the right thing by them.

In addition to providing important disclosure to our members, the process of pulling a transparency report together helps to remind us that we're guardians of our members' data and is a handy annual check-in on our own culture around privacy.

The process of transparency reporting influences our company culture and brand.

But it's not just businesses and their customers that could benefit from greater transparency. We believe that government agencies, which request information from businesses and other private organisations (such as NGOs), should also be regularly publishing the number of requests they make.

We think New Zealanders should have a right to know how, how often and for what reasons government agencies are requesting their information from businesses and other private organisations.

With an accurate picture of the extent of requests and releases being made, a healthy debate could take place on whether the existing checks and balances on government agencies, businesses and others adequately protect the privacy of individuals.

We think some sunlight on this issue would be a good thing.

Privacy Act reform

The Privacy Act came into force in 1993. That's nearly a quarter of a century ago, well before the internet got any real traction in New Zealand and some six years before Trade Me was founded. It goes without saying that the world has changed a bit in the last 24 years, especially in the way New Zealanders manage and use personal information.

We believe it's time New Zealand's privacy laws were freshened up.

In February this year the Privacy Commissioner, John Edwards, published **six recommended amendments** to the Privacy Act for the Government to consider.

If these recommendations are implemented, the OPC will receive further statutory powers to improve enforcement of the Privacy Act. We're cautiously supportive of this, but the devil is likely to be in the detail. There are some meaty recommendations which require lawmakers to balance the carrot to encourage compliance and the big stick of enforcement.

A good example is the Law Commission's recommendation to make it mandatory to report privacy breaches. Currently there is no statutory requirement for businesses, other types of private organisations, or government agencies to report a privacy breach (either to OPC or their customers).

Is this a good thing? We think reasonable arguments could be made both ways.

One of our core privacy values is to be straight up. This includes when privacy breaches occur. We reckon being transparent about breaches actually builds trust. But, while we would typically notify a member if their personal information was involved in a privacy breach, is it fair to impose a statutory requirement on us to also report this to the regulator?

On one hand, such a requirement could promote social responsibility, increase awareness that breaches happen, and assist in resolving issues that may not have otherwise been identified.

On the other, it could encourage businesses to withhold information they might normally have reported to the affected customer for fear of being pinged by the regulator. It's important to remember that while breaches are not good, not all breaches are equal.

We're looking forward to participating in the debate on whether the recommendations should become law. We understand the Government is still developing an exposure draft of a new Privacy Bill.

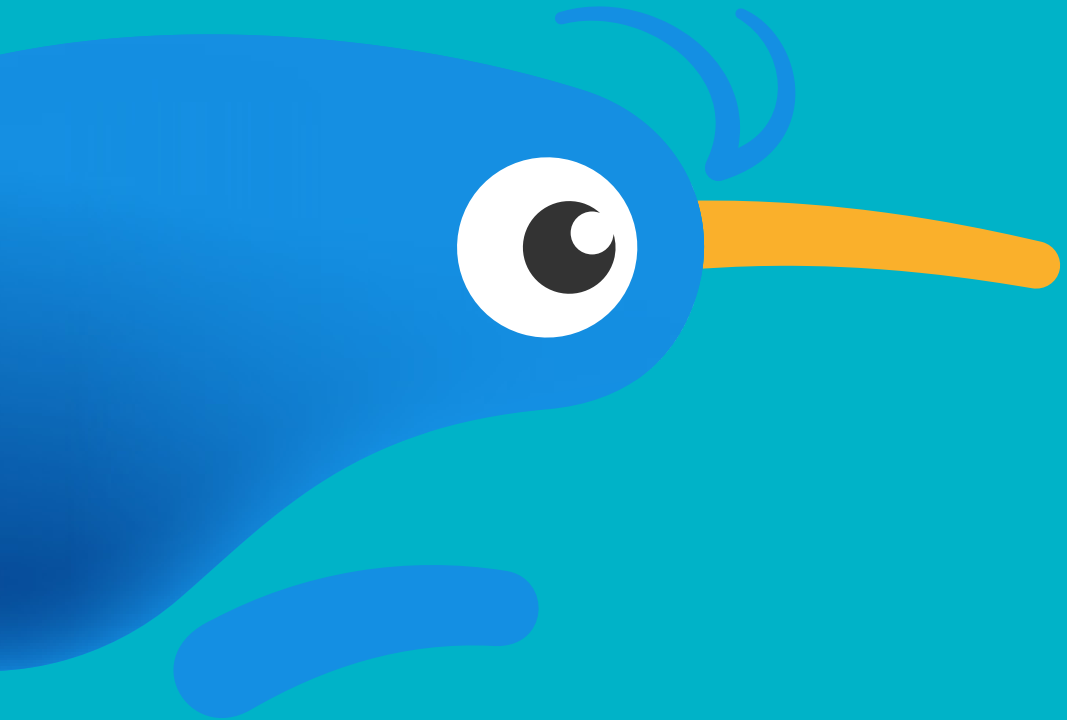
The stats

What stats are covered in this report?

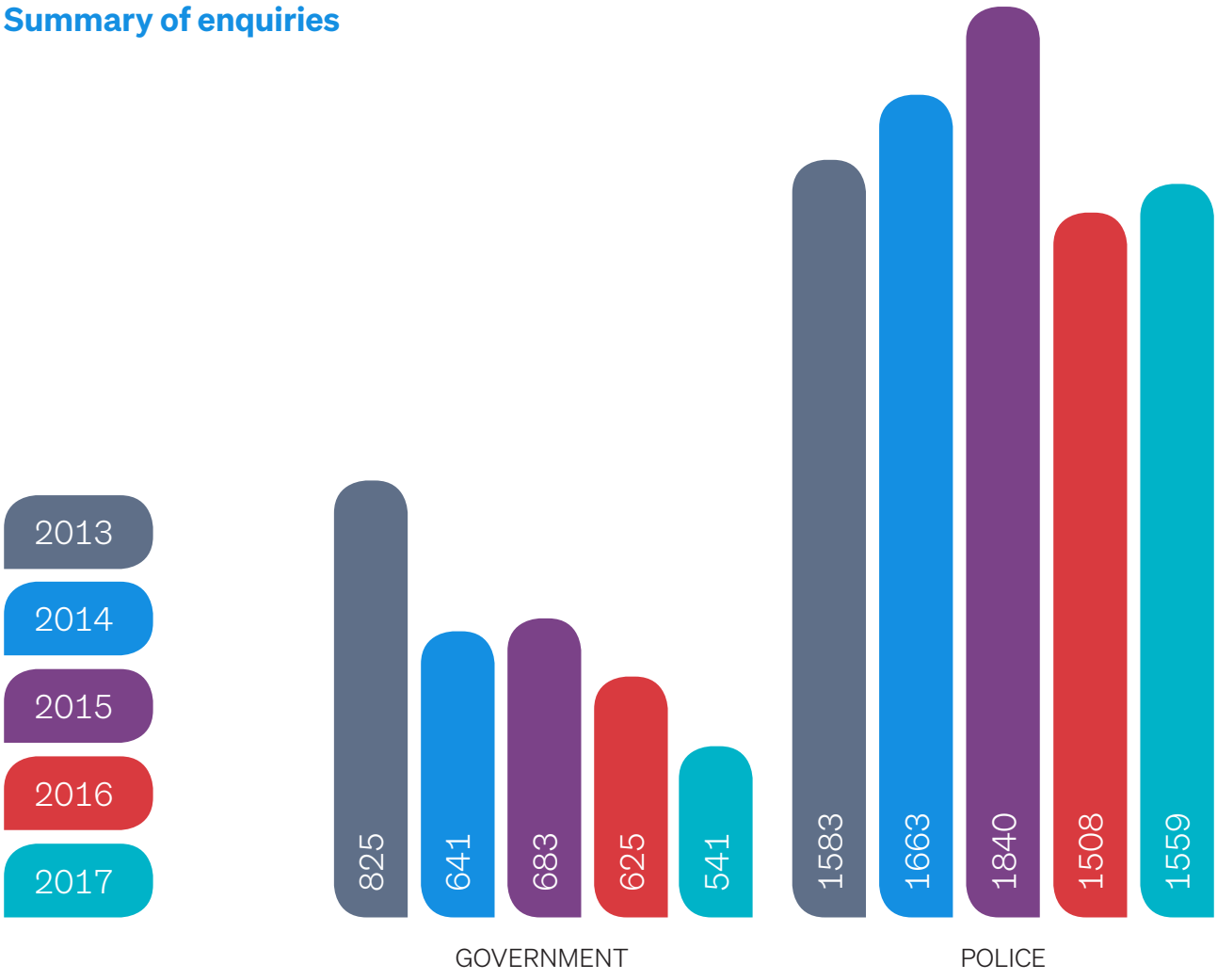
This report covers requests for, or releases of, members' personal information to government agencies between 1 July 2016 and 30 June 2017.

It also outlines the requests made to us in the reporting period by other members, and requests made by third parties where members have provided consent for their information to be released.

The following graph outlines the total number of requests we've received for members' information from government agencies. The data is split between the NZ Police and all other government agencies to provide more detail.



Summary of enquiries



New Zealand Police enquiries

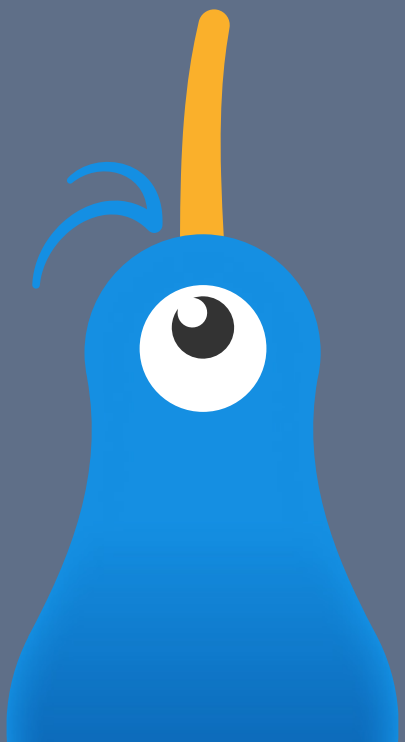
We work productively with the police to keep our site trusted and safe.

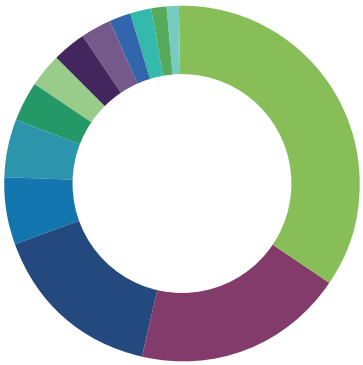
Police often help us ensure fraudsters (e.g. sellers that intentionally don't deliver items) are held to account.

Beyond the keyboards and smartphones, our relationship also helps keep local communities safe.

Breaking down the police enquiries during the reporting period:

- 8% of releases were made under a production order.
- 65% were made under the Privacy Act.
- 27% resulted in no release.





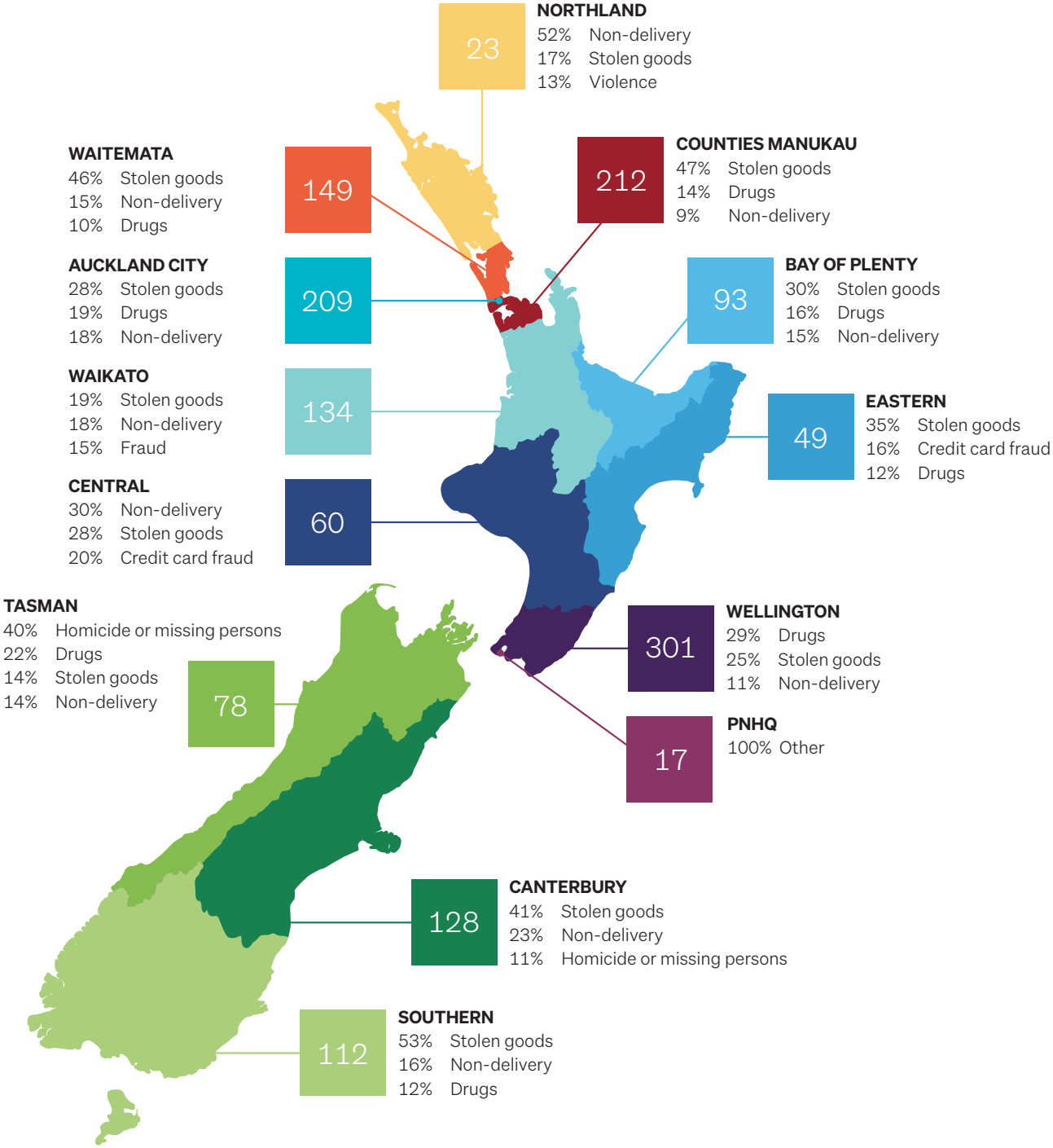
Police enquiry by type

This graph shows the subject matter of police enquiries received.

522	Stolen goods	**46**	Violence
288	Non-delivery	**42**	Sexual offending
241	Drugs	**31**	Firearms
90	Other	**27**	Proceeds of crime
81	Credit card fraud	**24**	Child exploitation
52	Fraud	**13**	Money laundering
47	Homicide or missing persons	**4**	Identity theft

Police enquiry by location

Top three classifications by volume for each region.



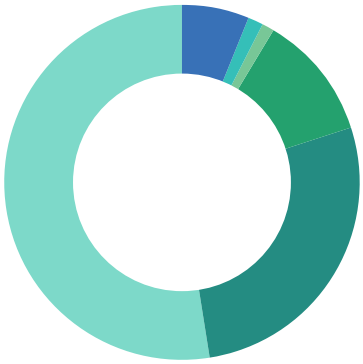
Government agency enquiries

Enquiries may be a request for member information, advice that a listing be withdrawn from the site without the need for the release of information, or a request for us to pass on educational information to a member.

During the reporting period, we liaised with 36 government agencies on 541 occasions:

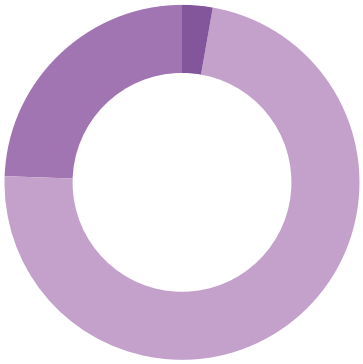
- 28% of those enquiries were compulsory information requests.
- 51% of enquiries resulted in information releases under the Privacy Act.
- The remainder resulted in no release of information.

Breakdown of three government agencies



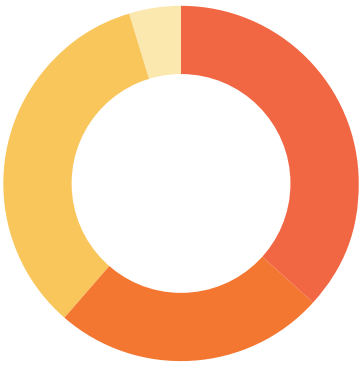
MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT

- **10** General
- **2** Companies Office
- **2** Immigration New Zealand
- **18** Insolvency & Trustee Service
- **44** Radio Spectrum Management
- **84** Worksafe New Zealand



MINISTRY OF HEALTH

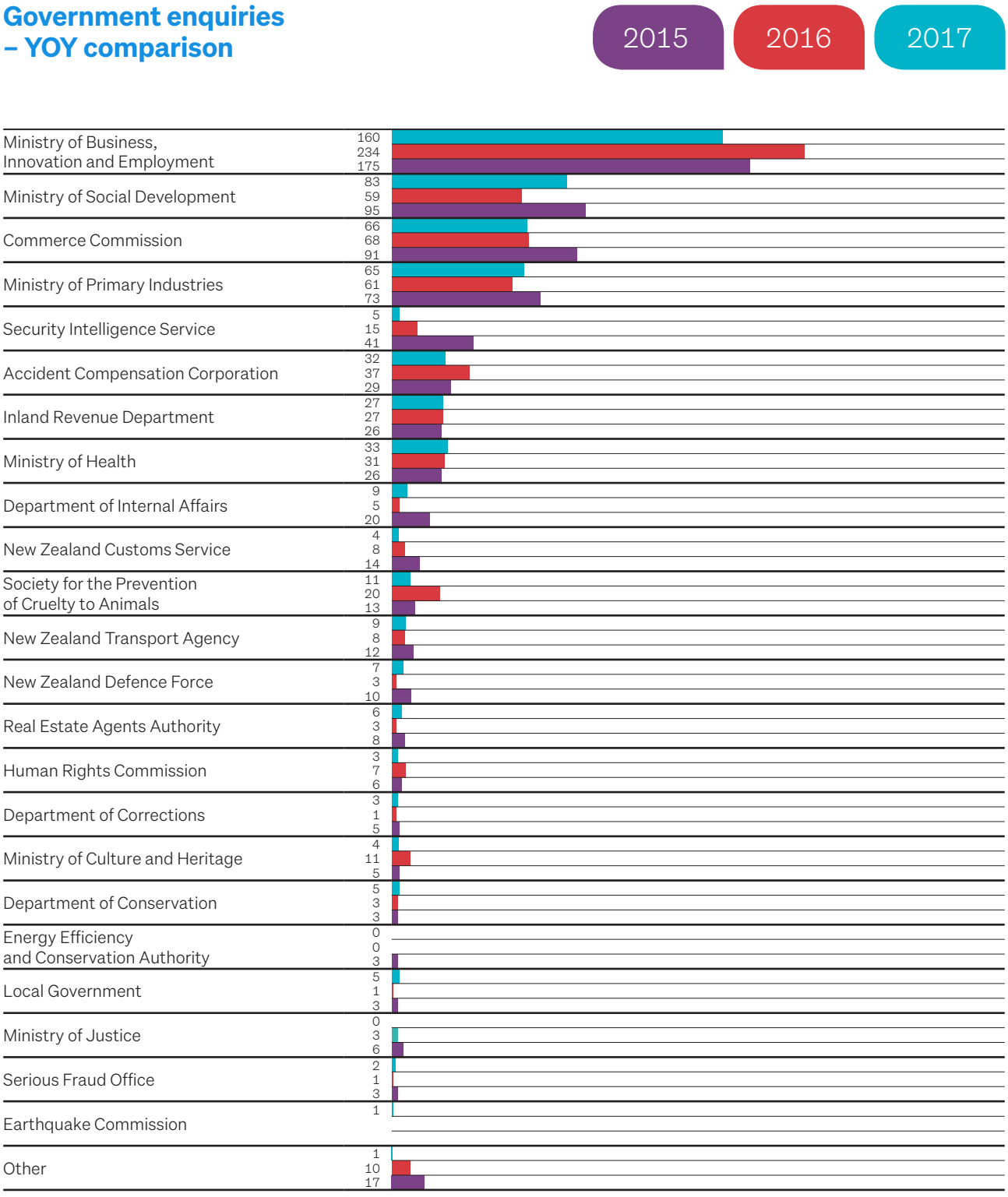
- **1** General
- **24** Laser pointers
- **8** Medicines



MINISTRY OF PRIMARY INDUSTRIES

- **24** Biosecurity
- **16** Fisheries
- **22** General
- **3** Agricultural Compounds

Government enquiries – YOY comparison



Push-backs

We work hard to ensure member information is released only when it's legal and we're satisfied it's appropriate. Sometimes we don't release information, even though we may have been permitted to under the Privacy Act.

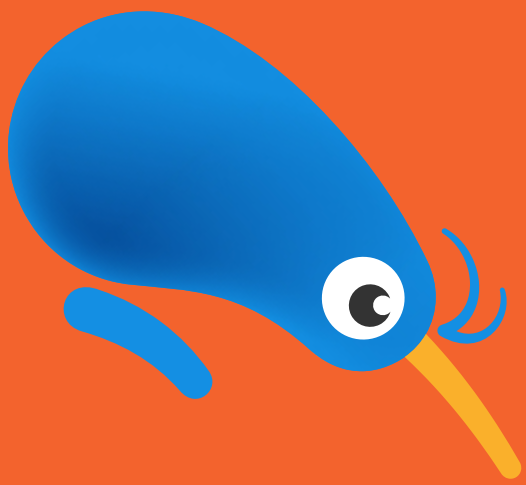
Following a request, we examine whether the information is required for the purpose stated by the requesting agency. If the scope of the request is too broad, we might 'push back' to ensure the information released is as sharply focussed as possible.

On the following page we compare our push-backs in the current period, against our prior reporting.

We have regular discussions with the police and government agencies to maintain a focus on quality requests. This increased focus results in the increased scrutiny of requests by our staff.

Police push-backs have decreased from 4.0% to 3.4% year-on-year in the 2017 reporting period, and government push-backs increased from 1.8% to 2.6%.

Police push-backs have decreased from 4.0% to 3.4% year-on-year in the 2017 reporting period.



Push back on

police enquiries

3.4%

Push back on

government enquiries

We pushed back on requests from government depts 2.6% of the time.

TYPE	PUSHED BACK
Drugs	26
Firearms	2
Fraud	5
Homicide or missing persons	1
Non-delivery	1
Other	7
Violence	2
Proceeds of crime	4
Stolen goods	6
2017 total	**3.4% 54**
2016 total	**4% 61**

AGENCY	PUSHED BACK
Commerce Commission	7
Department of Internal Affairs	2
Local Government	1
Ministry of Business Innovation and Employment	1
Ministry of Primary Industries	1
New Zealand Customs Service	1
New Zealand Transport Authority	1
2017 total	**2.6% 14**
2016 total	**1.8% 11**

Consented releases & Disputes Tribunal

Consented releases

Sometimes organisations contact us seeking information on a member's behalf (with the member's permission). Typically these requests come from insurers investigating insurance claims.

While we can make authorised disclosures under Principle 11(d) of the Privacy Act, we insist that the member's consent be in writing and signed.

To ensure the scope of the consent an individual is providing is always fully explained to them by the requesting agency, we introduced our own privacy waiver template this year as a mandatory step in the consented release process. Since we've introduced the waiver, requests for member information from the insurance industry have dropped from 72 to 20 – a rather drastic 260% decrease since 2015!

The introduction of a more informative and precise waiver has raised consumer awareness and caused insurance companies to be more circumspect with their requests, which is a great result.

While we can make authorised disclosures under Principle 11(d) of the Privacy Act, we insist that the member's consent be in writing and signed.

Disputes Tribunal

Members can choose to resolve trade disputes through the Disputes Tribunal. Under the Privacy Act, we release information relating to a trade if a member can demonstrate that tribunal (or court) proceedings are being reasonably contemplated and the information is necessary for those proceedings.

Members must provide us with a completed statutory declaration witnessed by a Court Registrar before we release any information.

The establishment of a dedicated Disputes team within Trade Me's Trust & Safety team in January 2017 has helped members resolve disputes before they even make it to a hearing.

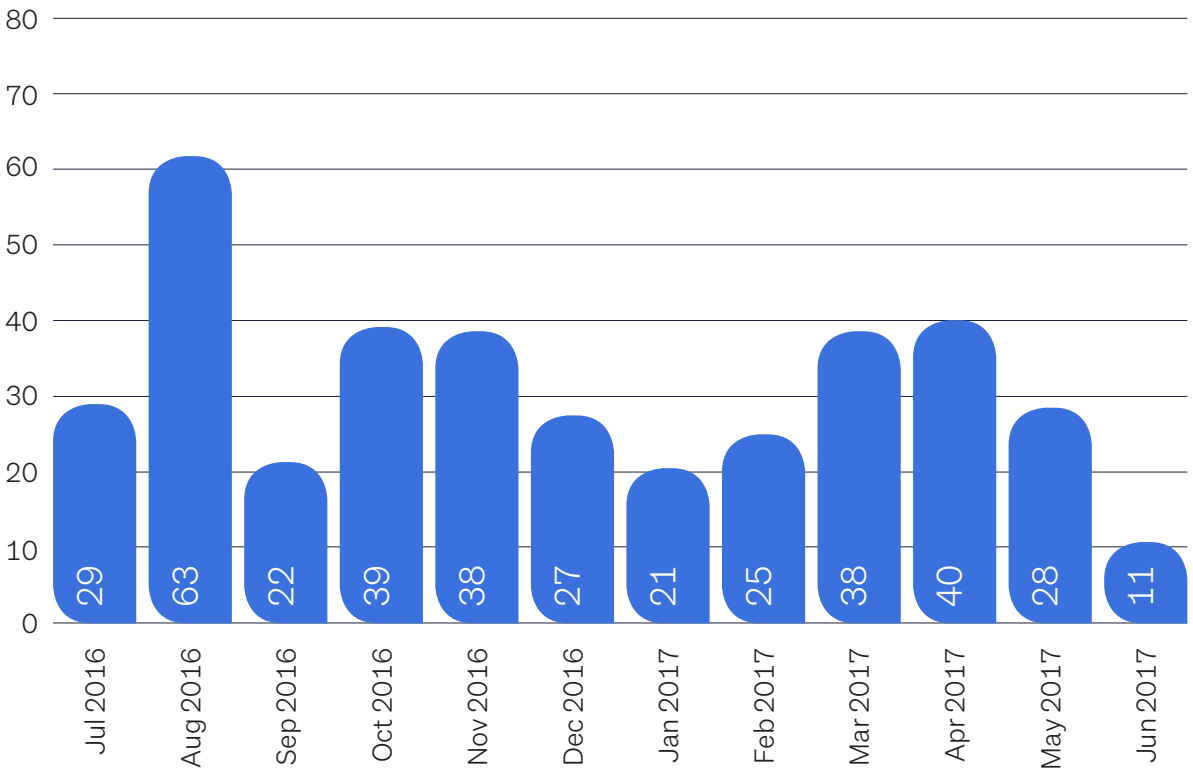
Because of this, and the introduction of our Buyer Protection policy, we've seen a 12% reduction in information releases required for Disputes Tribunal proceedings.

Members must provide us with a completed statutory declaration witnessed by a Court Registrar before we release any information.

Members requesting their own information

As our members become more aware of privacy, they continue to request their personal information in reasonable numbers. The graph below shows the level of requests by Trade Me members for their personal information under Principle 6 of the Privacy Act.

Member requests



Harmful Digital Communications Act

The Harmful Digital Communications Act came into effect in November 2015. Its goal is to deter, prevent and mitigate the harm caused to individuals by digital communications and to provide victims of harmful digital communications with a quick and efficient way of addressing it.

The Act applies to content made by Trade Me members on the site, such as in comments made on the message board or feedback.[1]

Usually if a member breaches the principles of the Act or their content is deemed harmful and/or offensive, they'll have breached our terms and conditions and we'll remove the content. However, in circumstances where we don't remove the content for breaching our terms and conditions, the Act prescribes a complaints process, sometimes referred to as the 'safe harbour' process.

The 'safe harbour' process, if triggered, requires us to use a prescribed format to notify the author of the content within 48 hours. Once notified, the author of the content must make a decision to stand by the content or have it removed.

Some commentators have expressed concerns that the prescriptive manner in which the Act requires online content hosts to contact content producers is intimidating. This may leave content producers feeling as though they have no choice but to remove content, even though that content may not breach the communication principles set out in the Act.

We agree with these concerns and, given the potential for the safe-harbour process to impact on the freedom of expression, we believe it's important for content hosts to publicly report the number of complaints they receive under the Act and how many times they have engaged the safe-harbour process.

In the current reporting period, five complaints were made to Trade Me under the Act and we chose to use the safe-harbour process for two of these pieces of content. On both occasions the content producers chose to remove the content complained about, despite our advice that the content was unlikely to breach our terms and conditions.

Harmful Digital Communications
Number of complaints: 5
Safe harbour exercised: 2

[1] For further advice on the HDCA, refer to Netsafe: https://www.netsafe.org.nz/advice/harmfuldigitalcommunications/

Frequently asked questions

What is meant by ‘enquiry’?

Enquiries cover a range of activity, such as:

- an information request where an agency has sought information about a membership (e.g. contact information or sales data)
- information that a listing may be in breach of the law (or our terms and conditions)
- highlighting an issue with a member which is then taken care of by us
- a request to pass on a message directly to members.

Does Trade Me need members’ permission to release information?

When joining Trade Me, we advise members via our terms and conditions that we release account and other personal information when we believe the release is appropriate to comply with the law, facilitate court proceedings, enforce or apply our terms and conditions, or protect the rights, property, or safety of our business, our users, or others. Our privacy policy provides more detail on this.

How safe is member data?

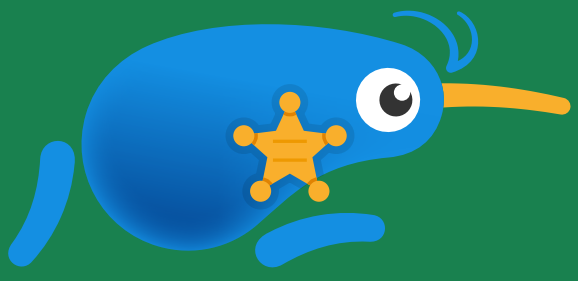
Very safe! We follow industry best practice methods to keep data safe. However, we are paranoid about this and are constantly working on ways to make it safer.

How often will this report be released?

We publish this data annually.

How do I access my own data?

This help page provides members with a list of the type of information we might hold about them, and who they need to contact in order to access this information.




trademe
Group Limited