trademe
Group Limited

Transparency Report 2018

Contents

Introduction

The last 12 months have been a busy time for Privacy at Trade Me. In addition to all the attention privacy and data sharing has been getting in the media, we've been busy reviewing and making changes to how we handle our customers' data. We updated our **privacy policy** on 6 June 2018, and as part of that we set out the principles we use to guide our decision making around data use.

These principles are:

- We will respect your privacy – our brand is built on trust and integrity.
- We're committed to being transparent and honest, so you know what we do with your personal information (including if something goes wrong).
- We use personal information to add value to your life.
- We avoid getting involved in anything creepy that could breach your trust.

To ensure we apply these principles consistently, we've also recently established a Data Governance Council made up of key Trade Me staff from around the business, including our Analytics and Trust & Safety team.

These principles also guide our continued commitment to transparency reporting.

Cambridge Analytica – raising the stakes

As with many privacy conscious companies, we've been following the recent activities of research firm Cambridge Analytica and their use of user data supplied by Facebook.

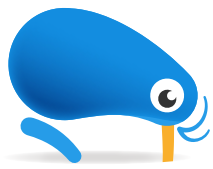
Whatever your opinion on Cambridge Analytica or Facebook's conduct, it's pretty clear that the issue has raised public awareness on data use, and prompted a higher-than-normal number of our users to contact us with requests under Principles 6 (requests for personal information) and 9 (requests for account deletion) of the Privacy Act. We detail this below.

While it creates work for our Trust & Safety team to respond to customer requests under the Privacy Act, it's a really important part of what we do. We employ a Privacy Operations Officer so we can quickly and efficiently respond to these requests.

The Alsford Decision

Given our stance on the usefulness and appropriateness of a voluntary release regime governed by the Privacy Act, we took considerable interest in the recent Supreme Court decision in Alsford.

The case involved the release of a consumer's consumption data by an energy company, after a request by the Police. The decision supports the right of agencies holding personal information to release that information to law enforcement where they have reasonable grounds to believe that it's necessary for the maintenance of the law.



The case makes it clear that the decision about releasing information sits with the agency holding that information, and that law enforcement agencies are responsible for providing sufficient information to those agencies, in order for them to decide whether there are grounds to release.

Agencies should not release if they don't have adequate information on which to make an assessment. If Trade Me is unsatisfied with the clarity or scope of a request, we'll demand further information to assess the merits of the request.

Firearms on Trade Me

In 2017 we entered into an arrangement with the New Zealand Police to make the sale of firearms on Trade Me safer.

Whenever a member buys, bids, or asks a question on a listing for a firearm or ammunition, we require that customer to provide their name and firearms licence number as they appear on their firearms licence. We then obtain confirmation from Police that the licence details provided are valid.

This lets us make sure the customer attempting to buy the firearm is the same person as named on the Trade Me membership, and that the person is legally entitled to purchase firearms. This process significantly restricts the ability of unlicensed buyers to use Trade Me to attempt to obtain firearms or ammunition illegally.

The ability to receive a yes/no response in relation to a Firearms Licence number from the Police National Firearms Database is based on customers consenting to us checking them. Customers input their own firearms licences – we don't collect or disclose this without the consent of the user. You can read more about our process in this **blog post**, and along with the **Office of the Privacy Commissioner's FAQ**.

The Privacy Bill

There's been a lot of commentary on the Privacy Bill introduced into the House and making its way through the Select Committee stage.

We're really happy to see progress on updating the Act. There's lots to like about the Bill as it stands, and we have a few suggestions on making it better.

Here are some of the highlights from our submission on the Bill:

- We think that the Bill could include higher penalties for offences under the Act and additional enforcement powers.
- We reckon the Privacy Commissioner should be able to require that agencies demonstrate that they comply with the Privacy Bill, without the Commissioner having to receive a complaint about the agency.
- We think the Bill needs greater provisions to protect against re-identification in anonymised data.
- We also think that other significant privacy issues need a full review and consultation process, to ensure that our new privacy law is fit for purpose and up to date.

Check out our Trade Me **submission on the Privacy Bill.**

Harmful Digital Communications

Sometimes people aren't very nice to each other on the internet. We see this on Trade Me occasionally, in particular when things have gone wrong with a trade and feedback gets a bit fresh, or when our messageboard users forget how to behave like adults.

Typically we deal with potentially harmful content under our terms and conditions because most of the time it's obvious when conduct crosses the line and should be removed. However, in rare circumstances, Trade Me could be the host of content posted by one person and considered harmful by another. If we don't agree that the content should be removed, a complainant has the option to make a complaint to us under the Harmful Digital Communications Act.

By following the prescribed process under the Act, we avoid liability where a publisher refuses to remove potentially harmful content. The Act's safe harbour process basically means that where we promptly talk to the the content publisher to confirm they stand by what they've posted and they don't remove it, they are responsible for any potential harm that comes from it.

We've not had to exercise the safe harbour provision in this 2018 reporting period.

PRIVACY TRUST MARK
NOHO MATATAPU

Privacy Trust Mark

As a final note before we get into the stats, as part of Privacy Week 2018, the Office of the Privacy Commissioner launched a new initiative – the **Privacy Trust Mark**. The award recognises excellence in privacy-friendly products or services.

We were really proud to be one of the two inaugural recipients of the award, for our work producing transparency reports over the last five years.

The statistics

In our 2017 Transparency Report, we talked about the difference between agencies releasing information voluntarily under the Privacy Act and being compelled to do so by an enforcement agency (e.g., subject to a search warrant or production order).

For the second year in a row we are reporting on the number of releases that we make under the Privacy Act, versus releases that are compelled under legislation by public sector agencies.

This year, 4% of the requests we received resulted in us releasing information pursuant to a Production Order, and 69% of requests we received resulted in us releasing information under the Privacy Act. This is a decline in Production Orders since last year, where 8% of requests resulted in a release under a Production Order.

Last year, 27% of requests from the New Zealand Police resulted in no release. This year, that number is down slightly to 25%. The reasons why a request may result in no release of information include:

- the information sought does not exist or cannot be found,
- the request relates to an item that has been misidentified as being stolen and therefore no release is done,
- the information is no longer needed, or
- we decline to release information voluntarily under the Privacy Act.

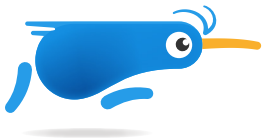
This year we've seen a decline in releases to the New Zealand Police (down 13.6% on last year), as well as a decline in releases to other public sector agencies (down 17.4% on last year).

Summary of enquiries

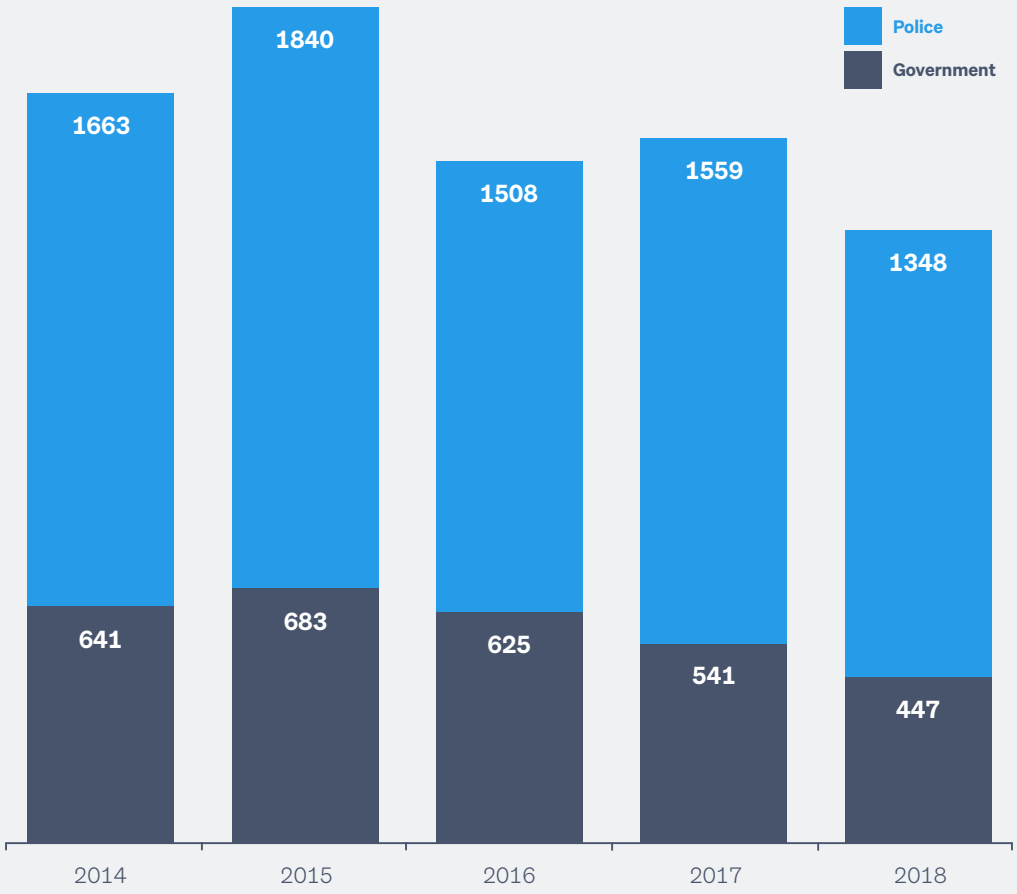
This report covers requests for, or releases of, customers' personal information to government agencies between 1 July 2017 and 30 June 2018.

It also outlines the requests made to us in the reporting period by other customers, 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 customers' information from government agencies. The data is split between the NZ Police and all other government agencies to provide more detail.



Summary of enquiries



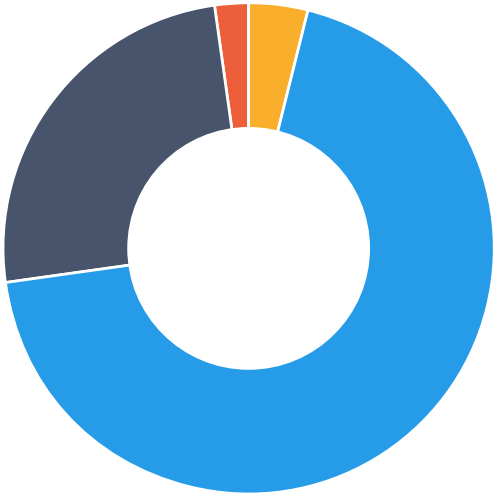
New Zealand Police enquiries

We work with the New Zealand 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.

New Zealand Police enquiries breakdown



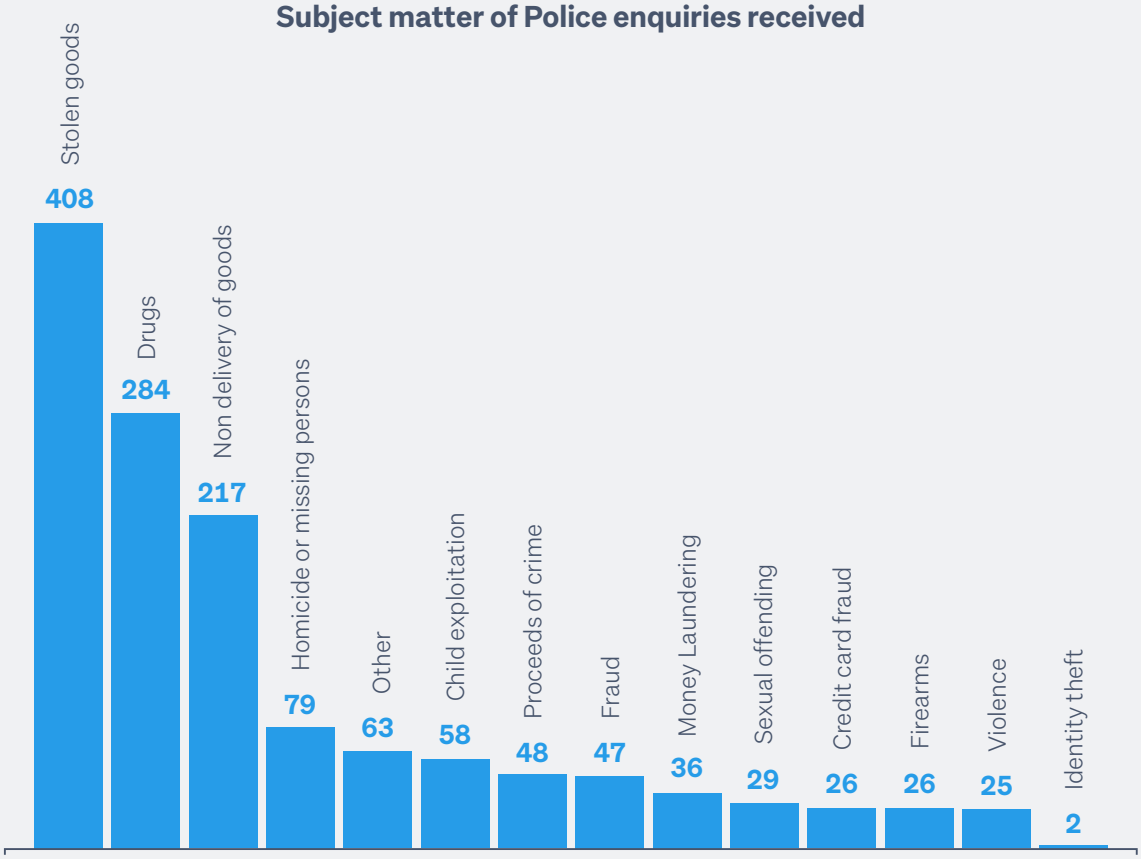
4%
releases made under a production order

69%
were made under the Privacy Act

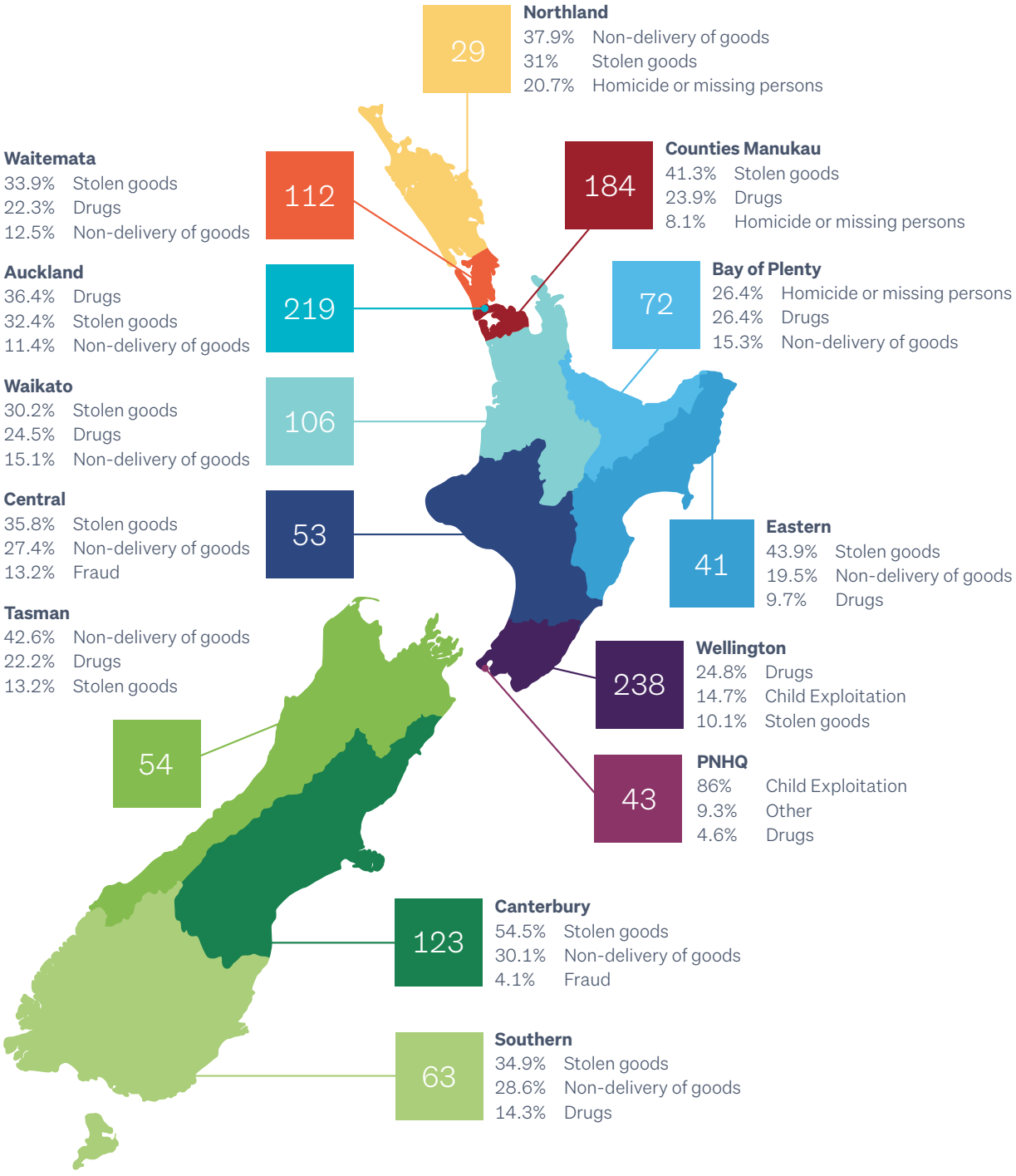
25%
enquiries resulted in no release

2%
were incomplete requests

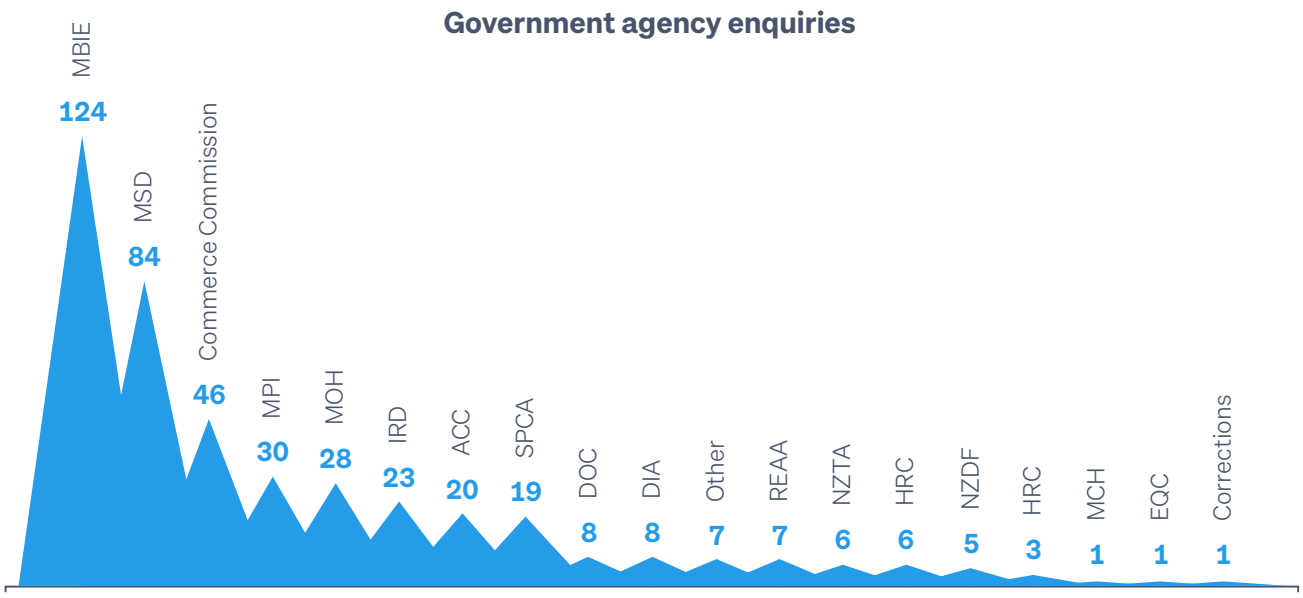
Subject matter of Police enquiries received

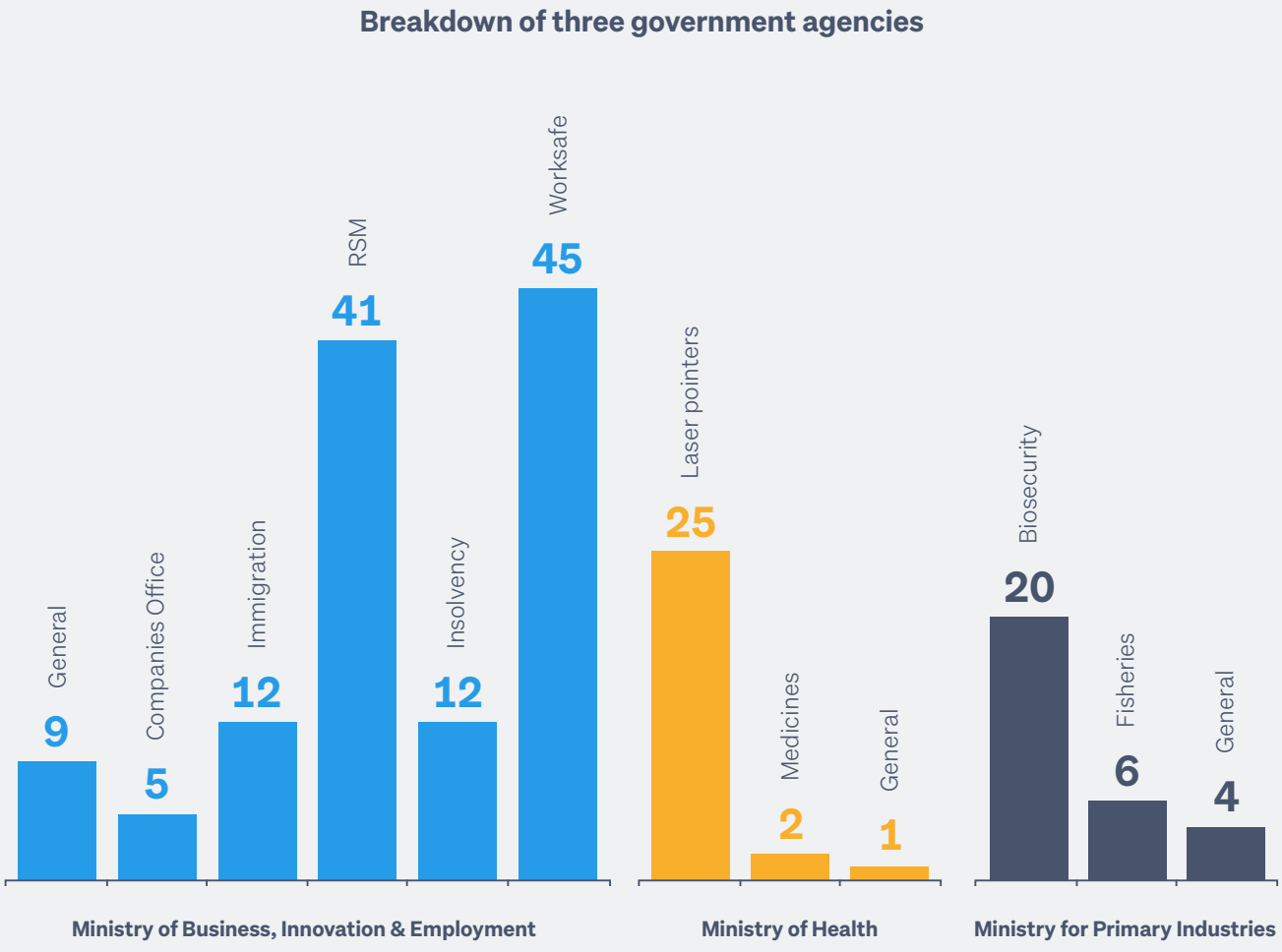


New Zealand Police enquiries by location



Government agency enquiries





Push backs

We want to make sure our customers' personal information is only released to government agencies and the New Zealand Police when it's legally requested of us and we're satisfied it's appropriate.

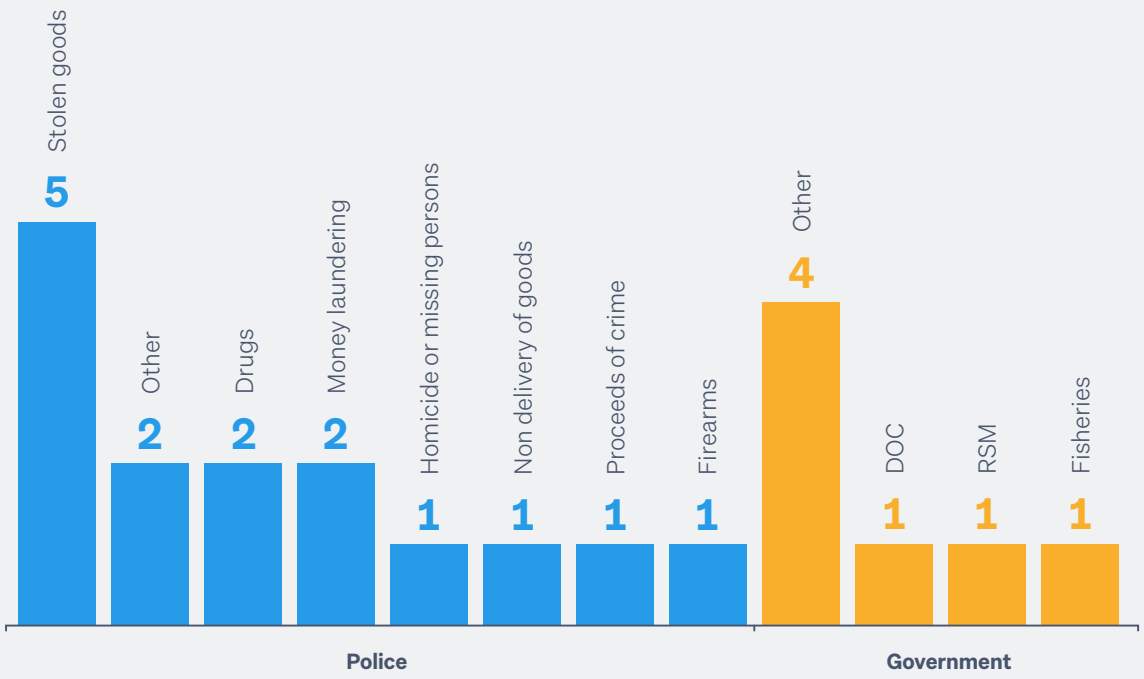
We don't release information, even though we may have been permitted to under the Privacy Act, if we feel something's not quite right.

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. This is especially so if we are choosing to release under the Privacy Act at our discretion.

We have regular discussions with the New Zealand Police and government agencies to maintain a focus on quality requests.

Police push backs have decreased from 3.4% to 1.1% year-on-year in the 2018 reporting period, and government push backs decreased from 2.6% to 1.6%. We believe this reflects an increase in the quality of requests received.

Subject matter of push backs received



Consented releases & Disputes Tribunal

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

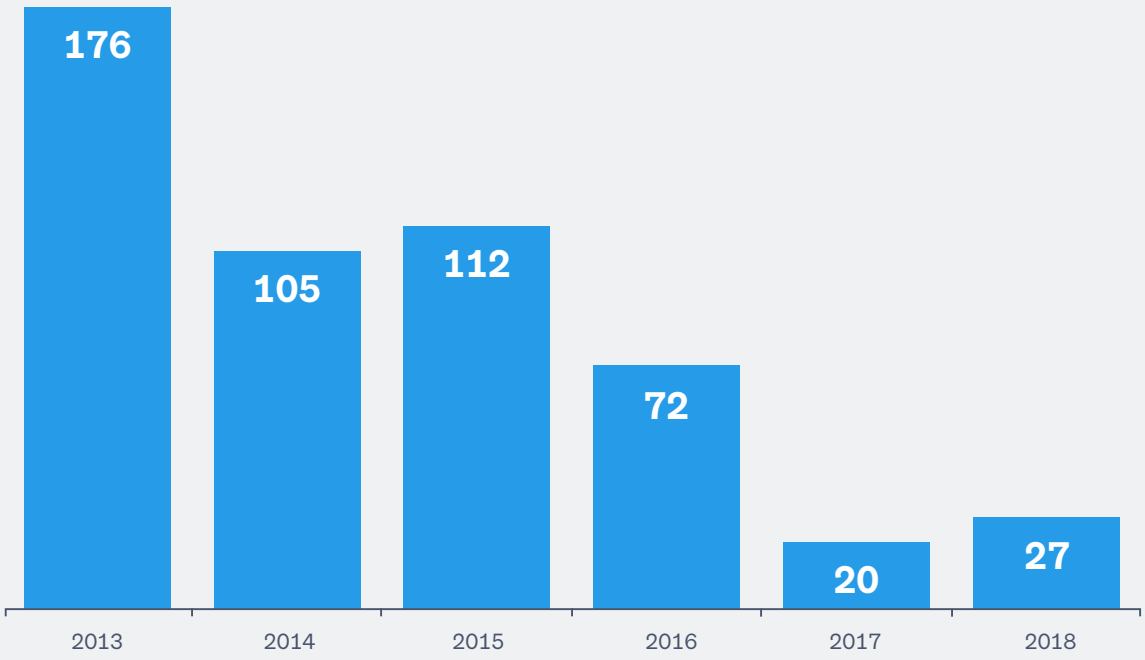
While we can make authorised disclosures under Principle 11(d) of the Privacy Act, we insist that the customer's consent be in writing and signed.

To ensure the scope of the consent an individual is providing is always fully explained to them by the requesting agency, we created our own privacy waiver template last year, which is now used as a mandatory step in the consented release process.

Since we introduced the waiver, requests for customer information from the insurance industry have dropped dramatically to around one-third of what they were five years ago.

The introduction of a more informative and precise waiver has raised consumer awareness about what they're consenting to, and has helped to ensure insurance investigators are careful with their requests, which is a great result.

Releases to Insurance Investigators under Privacy Principle 11(d)

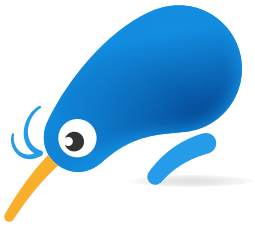


Customers can choose to resolve trade disputes through the Disputes Tribunal.

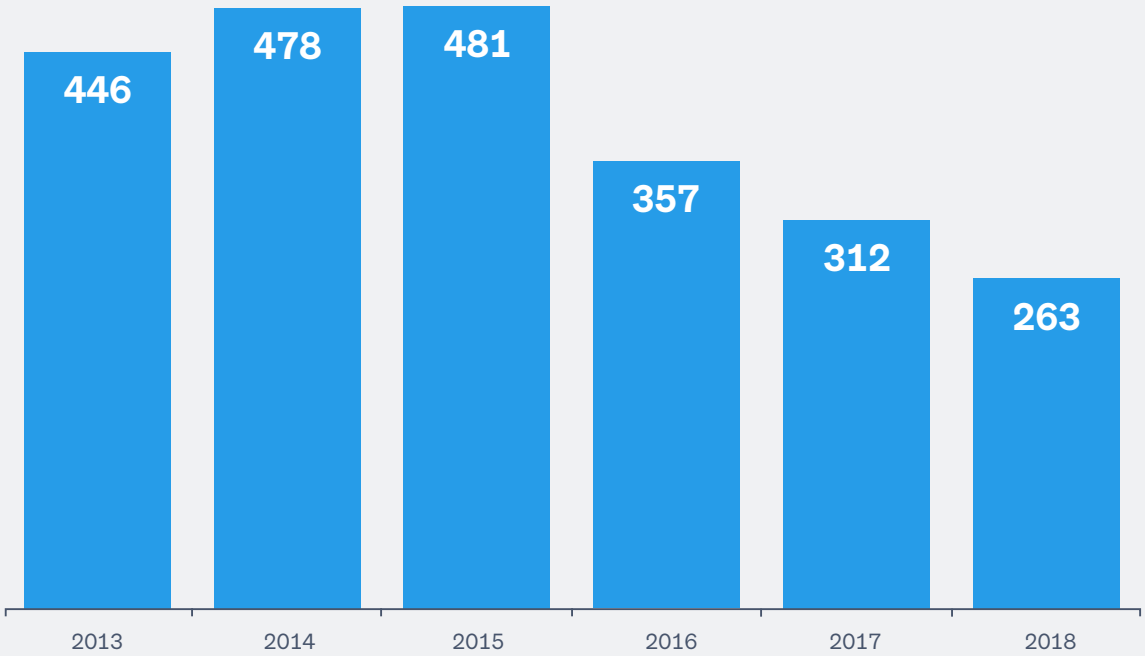
Under the Privacy Act, we release information relating to a trade if a customer can demonstrate that tribunal (or court) proceedings are being reasonably contemplated and the information is necessary for those proceedings.

Customers must provide us with a completed statutory declaration witnessed by a Court Registrar before we release any information. The information released is usually a name and an address, so a notice of hearing can be served on the other party.

This year we observed a 16% reduction in the number of statutory declarations received. This is likely to due to the fine work of the Trust & Safety team, which works hard to resolve disputes before needing to proceed to the Tribunal. Our **Buyer Protection programme** (which was introduced last year) has also meant that many customers have been covered under the programme and therefore have had no need to go to the Disputes Tribunal.



Statutory declaration requests



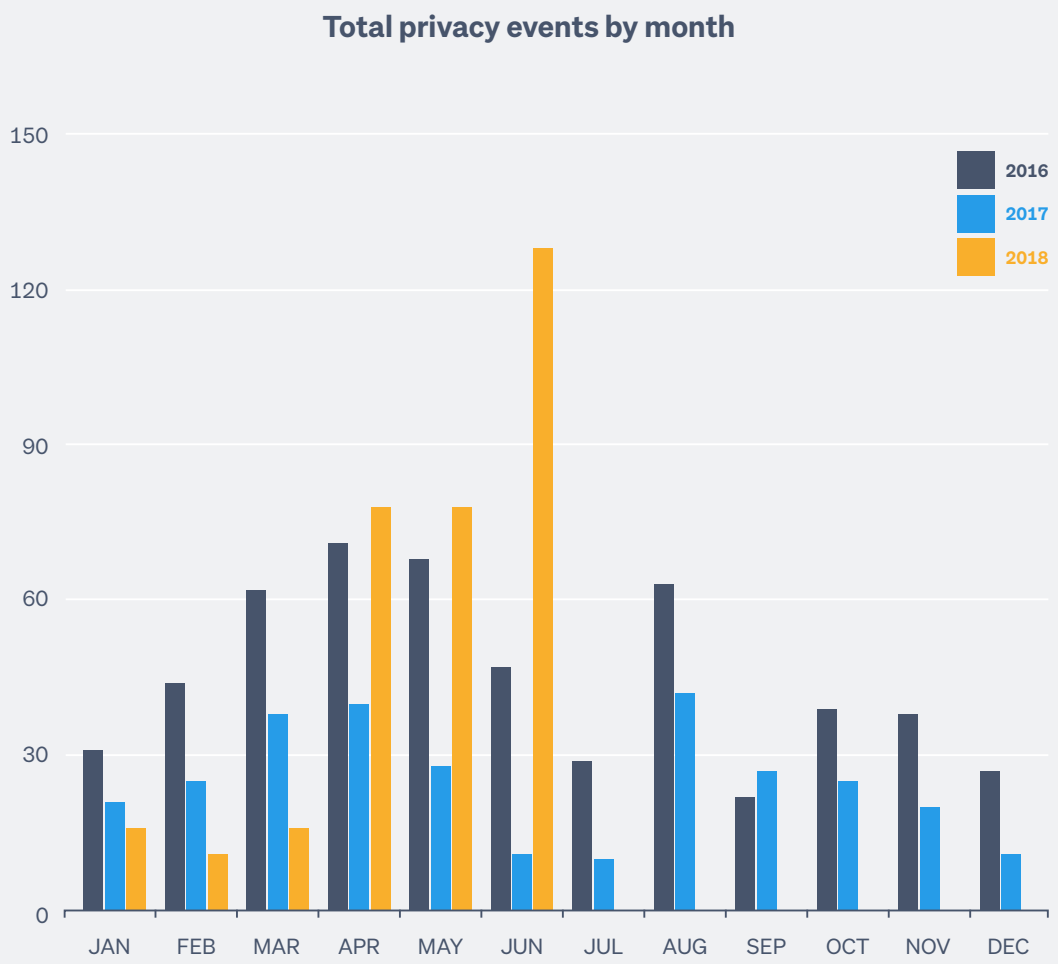
Total privacy events by month

On 17 March, the New York Times and the Guardian broke the news about the Cambridge Analytica/Facebook information sharing scandal. We believe that the high profile media coverage and public discussion that followed was the reason for a spike in the number of Principle 9 requests.

Principle 9 of the Privacy Act states that agencies shouldn't retain information for longer than is required for the purposes for which the information may lawfully be used.

Individuals request their personal information be deleted under Principle 9. You can **learn more here** about requesting to delete your information.

We also saw an increase in contact from members about privacy after we announced the changes to our Privacy Policy on 6 June, and that is reflected in the number of requests we received in June. We reckon that the **GDPR** (the new EU privacy law) coming into effect and the heightened awareness of privacy due to the Cambridge Analytica/Facebook media coverage has resulted in greater public awareness of privacy, which in our opinion can only be a good thing.



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,
- a request from an individual who needs information that Trade Me holds for Court or Tribunal proceedings.

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.

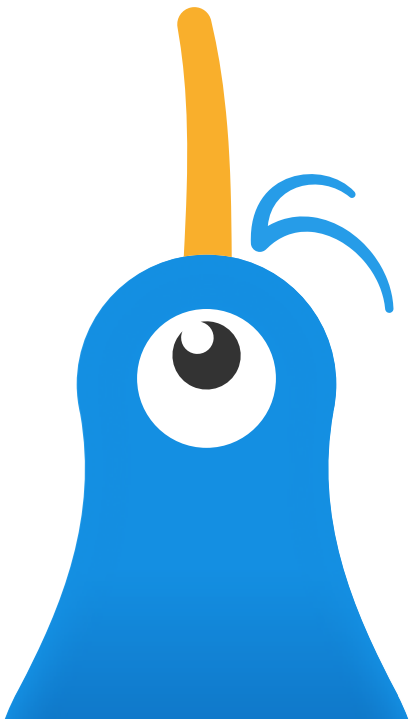
Does Trade Me need members' permission to release information?

When joining Trade Me, we advise members via our Privacy Policy terms and conditions that we release account and other personal information when we believe the release is appropriate for legal compliance or law enforcement purposes, to facilitate legal processes, to enforce or apply our terms and conditions or policies, or to protect the rights, property or safety of us, our Users or others. 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 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 how to best get in touch with us to access it.



trademe
Group Limited