Privacy Awareness and Engagement in Aotearoa New Zealand

Insights Report May 2022

Privacy Commissioner
Te Mana Mātāpono Matatapu

www.privacy.org.nz

Introduction

Privacy is the foundation of trust.

If you hold personal information, you must protect the privacy and mana of those who have entrusted it to you. As well as meeting your legal obligations, taking care of New Zealanders' personal information helps ensure people maintain trust and confidence in your organisation.

Every two years, we carry out a snapshot survey of New Zealanders and privacy – their levels of concern about privacy issues, their trust in those holding personal information, and their awareness and use of their privacy rights.

The global pandemic has seen significant change in the way we live. We share more of our personal information to increase overall community health benefits, through contact tracing and other Covid-related actions. We increasingly access goods and services online, from medical appointments to banking to grocery orders – we have to trust things will be ok and our information is safe, or we'll miss out on the things we need or want.

As part of our commitment to being a good Te Tiriti partner, this year a Māori booster sample was also included in our biennial survey to provide more depth to findings among Māori. It is too soon to draw any conclusions from these results given the statistical limitations of a sample this size and the fact that it is the first time we have boosted the sample. The results will be a useful input into conversations we intend to have with Iwi/Māori over the coming year, to help us understand how we can best improve privacy outcomes for Māori.

This insights report brings together highlights of the biennial survey and our own internal insights reporting to provide a fuller picture of what New Zealanders think about in relation to privacy in New Zealand, and how they utilise their privacy rights.

Our key messages:

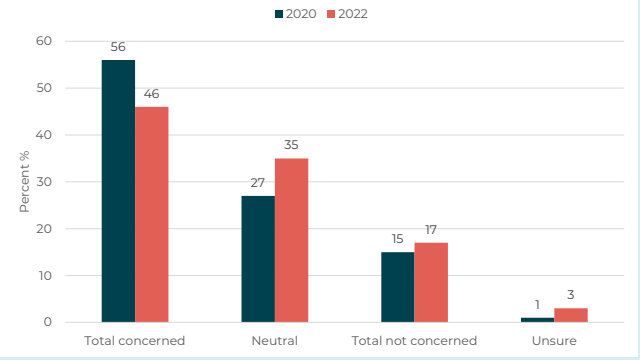
- Privacy concerns depend on the situation
- People's awareness of their right to access their own information is limited
- Most privacy breaches are avoidable
- OPC is here to help agencies and individuals when something has gone wrong

Insight 1

Privacy concerns depend on the situation

In 2022 the level of concern about individual privacy and protection of personal information has fallen to similar levels observed in 2001 after a surge in the 2010s. Just under half declared they were concerned compared to just over half in 2020. More than half of New Zealanders care about specific privacy issues that we think matter.

Changes in concern levels from 2020 to 2022



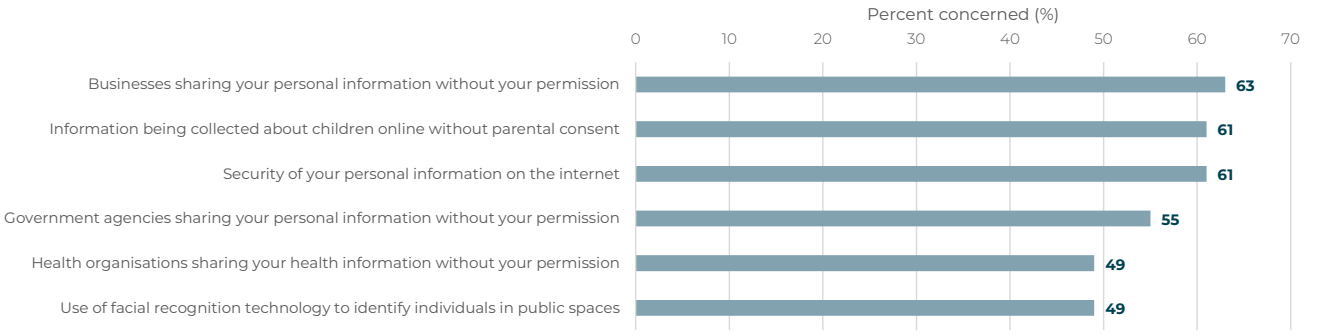
*Note: Due to rounding, the figures for each year do not add up to 100%.

The leading privacy issues of concern were 'businesses sharing personal information without your permission', 'information collected about children online without parental consent' and 'security of personal information on the internet'. Six out of ten New Zealanders were concerned about each of these issues.

Our research shows that people have become significantly less concerned about the security of their information on the internet over the last few years. However, InternetNZ's 2021 research found the opposite. Further investigation is required into the drivers of these apparently conflicting results. Is sharing of personal information online so ubiquitous that people no longer feel like they have a choice? It could be that people are genuinely more comfortable that their privacy is being protected or it could be that in the midst of Covid-19 it has dropped off their radar.

There has been ongoing media coverage of cyber-security issues and major stories about social media monitoring and tracking. This is having an impact on the way people think about who they give their information to. Just under half of New Zealanders say they would avoid doing something on the internet (such as

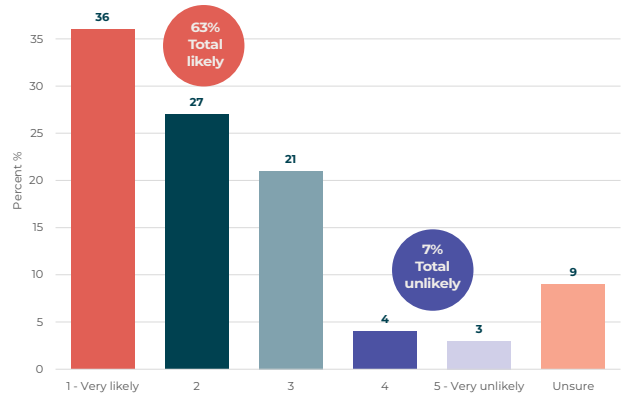
Privacy issues of concern (AKR Survey)



browsing or making a purchase) due to concerns that their online activity is being tracked.

Some other indications that New Zealanders care about their privacy are that six in ten people surveyed said they would be likely to change service providers if they heard their current provider had poor privacy practice.

Q: How likely would you be to consider changing service providers if you heard they had poor privacy and security practices?
(AKR Survey)



Interestingly, less than a third of people say they always read the privacy statements of organisations or services they are signing up to, with over a third saying that it depends on the context. These statements are a key mechanism for ensuring that people are well-informed about why their personal information is being collected and how it will be used and cared for.

Organisations can help people understand what is happening to their personal information by making privacy statements as clear and concise as possible. Our online Privacy Statement Generator tool makes it easy for agencies and organisations to create their own.

Case study: From identified issue to systemic solution

In some situations, the power imbalance between people and agencies is such that even if people are not comfortable with the way that their personal information is being collected and used, they are not in a position to do anything about it. The rental sector was an example of this. In early 2021, we saw that some property management agencies were asking for very detailed information from prospective tenants as part of their selection process, while others were using public forums to compile lists of so-called 'bad tenants'. Recognising that tenants had little power to challenge those responsible for their housing security, we took a proactive stance to protect the rights and privacy of tenants and prospective tenants.

We developed new guidance for tenants, landlords, and others in the rental accommodation sector to clarify what information may be requested at every stage of the rental process, as well as a reporting tool for tenants to confidentially email us about their rental experiences. We also launched a new monitoring and compliance programme to ensure that rental agencies and landlords stay on the right side of the Privacy Act. There are promising early signs that this has resulted in a significant reduction in the amount of personal information being collected from people who are looking for a rental home – a good outcome for privacy.

Insight 2

People's awareness of their right to access their own information is limited

Around half of survey respondents know they have the right to request their information under the Privacy Act. The Privacy Act is extremely clear – you have the right to your own information, and to have it corrected if it is wrong. One in ten survey respondents have requested a copy of their personal information from an agency or organisation.

The consequences of making it difficult for people to find out what personal information you hold about them, or of holding inaccurate information can be devastating. As an agency, you may lose the trust and confidence of your clients, customers, and stakeholders, but your clients may lose much more. Accuracy of personal information also ensures that agencies are making decisions with the full picture in front of them.

Questions about getting access to their own information, and the way their information is being shared or disclosed, are consistently the issues that our call centre gets most enquiries about from individuals.

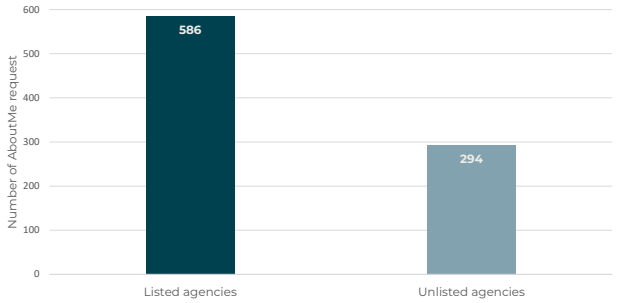
Likewise, over 80% of all complaints received by OPC are related to issues with people getting access to their own information – that they were unable to access it, that it was wrong or missing information, that it took too long, or it was refused.

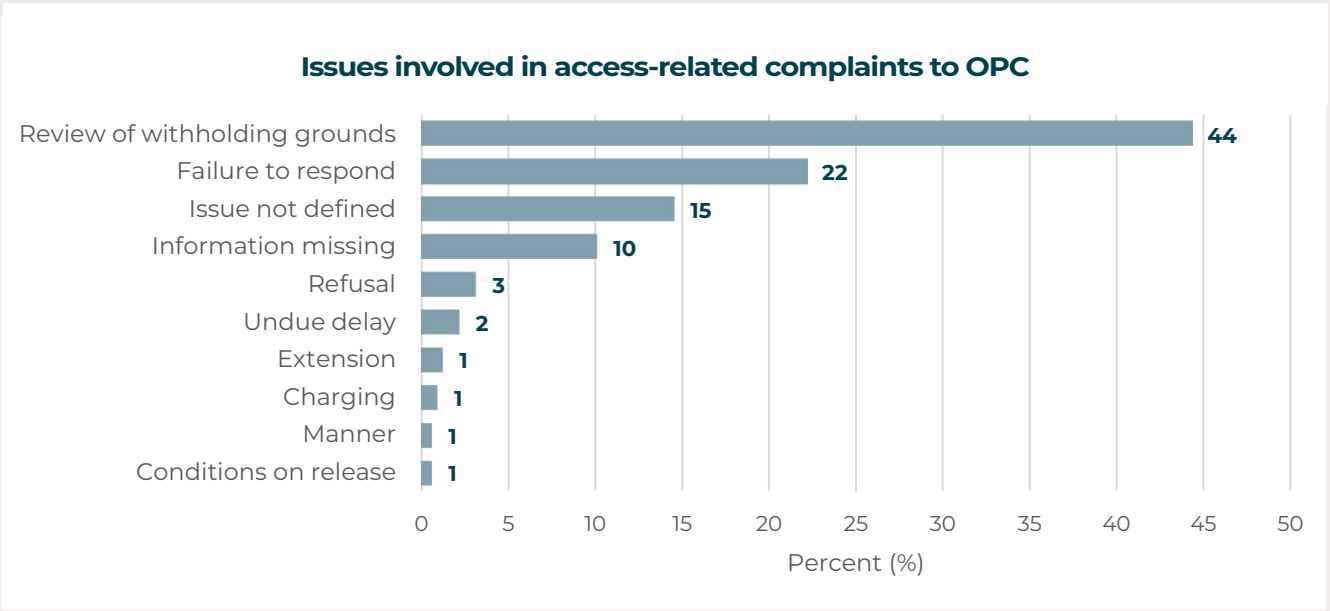
OPC and our suite of tools can help people access their own information and help rectify it if the information held about them by an agency is inaccurate.

Through our AboutMe tool, people are able to apply direct to agencies for their own information. This is likely a small percentage of total access requests made as many requests will be made direct to the agency concerned without the use of our tool.

Ensure you have good systems and processes to make sure that it is easy to give a timely and accurate response to access requests. It's the law but also good for trust and confidence.

Uptake of AboutMe tool
(year to 31 March 2022)





Case study: "Not my debt"

A debt management company mistakenly associated a man's name with the debts of another person for more than two years. The error meant any organisation querying the man's credit history would find records indicating he had unpaid debts.

In 2018, the man was alerted to the mistake after his request to have utilities connected at his property was declined by a provider due to a debt against his name. The man contacted the debt management company to inform them it had the wrong person. He demonstrated that he had a different middle name to the debtor and had never lived at the address the company had associated him with.

Despite the man repeatedly contacting the debt management company asking them to correct its mistake, two years later it had still failed to rectify the issue, resulting in the man being declined access to services and credit.

After the man complained to us, the company took responsibility for the mistake and agreed to provide a substantial confidential settlement to the man for the harm he had suffered.

This case is a reminder of how important it is for organisations to keep accurate records about their customers or clients. It also highlighted why organisations should have robust processes for investigating and actioning complaints.

Insight 3

Most privacy breaches are avoidable

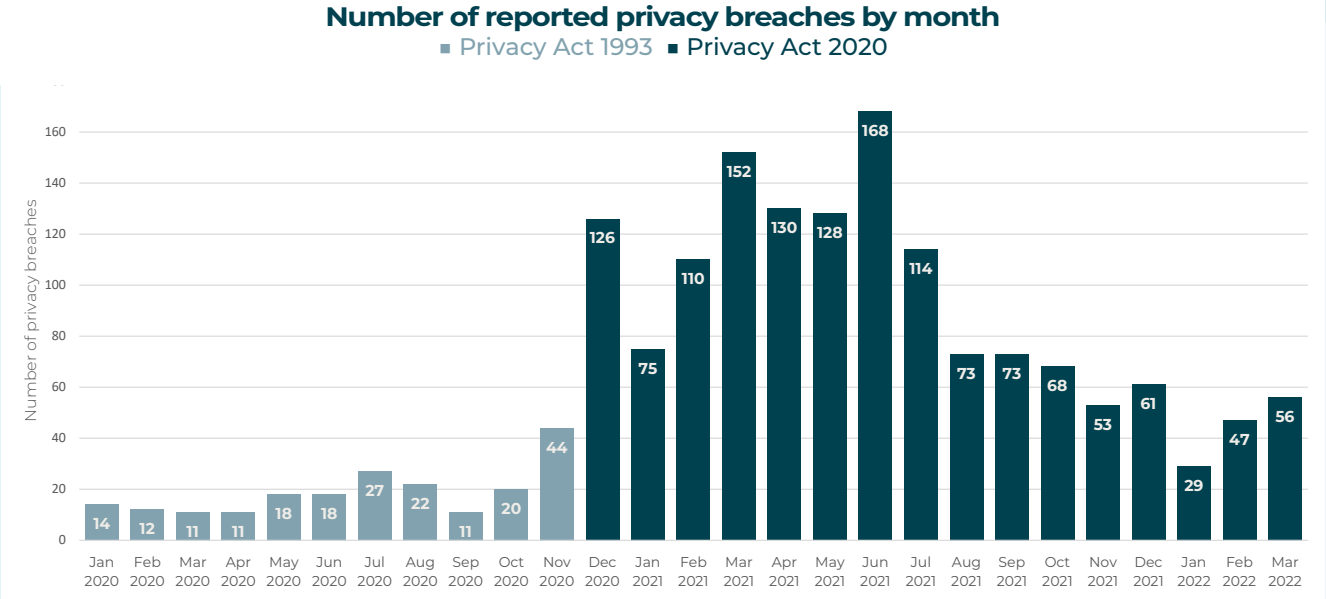
Privacy breaches continue to happen and continue to affect the lives of New Zealanders. Over six in ten New Zealanders would consider changing provider if they hear of poor privacy practice – it is in your organisation's best interest to ensure that you are protecting peoples' personal information. A breach of privacy is a breach of trust, and clients and customers have long memories.

After an initial rise in breach notifications to OPC after the launch of the new Act and the introduction of mandatory reporting of serious breaches, the total has dropped. However, it is still too soon to discern whether this is due to improvements in privacy practice or failure to report breaches as the new requirements are no longer front of mind.

Health Care and Social Assistance is by far the industry reporting the highest number of serious breaches, followed by Public Administration and Safety.

Human error remains the biggest cause of serious privacy breaches. Email error continues to account for over a quarter of those breaches, with other causes including accidental disclosure of sensitive personal information, data entry errors, confidentiality breaches, redaction errors, and postal and courier errors. These are breaches that can and should be minimised through good internal privacy practice and processes.

A common misconception is that a privacy breach only occurs where personal information is inadvertently shared to, or inappropriately accessed by, someone external to the agency. That is not the case. So-called 'employee browsing' – employees browsing personal records they have no work need to look at or



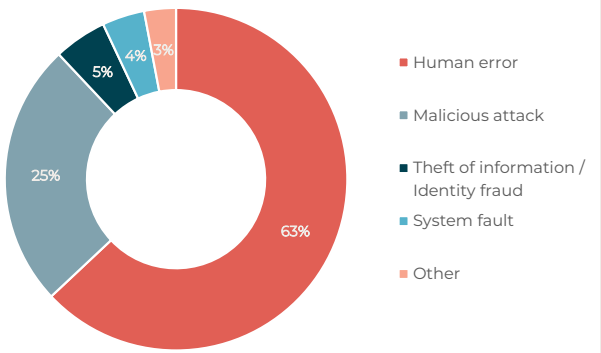
looking up the records for friends or family members - may be HR or professional conduct issues, but they are also privacy breaches and need to be avoided.

Employee browsing and internal sharing of information may account for only a small number of serious breaches reported to OPC, but they have the potential for significant negative impacts on an organisation's reputation. Staff need to know what they should, and shouldn't, be looking at within the scope of their work. Internal privacy breaches such as employee browsing also need to be reported to OPC, and we suspect that these breaches are being under-reported.

Whether a privacy breach is caused by accident or malicious intent, the impact on those affected can be devastating. All organisations, whether private or public sector, large or small, need to ensure that the information entrusted to them by their employees, members and clients is gathered appropriately and protected from loss, accidental or unauthorised disclosure, access, use or modification.

Unfortunately, many breaches resulting in serious harm occur because previous internal errors weren't deemed serious enough to be properly rectified. Examples are where a previous incident wasn't identified as a privacy breach, or the outcome of the breach wasn't considered serious enough to result in further action. If your organisation has a breach or near-miss, make sure that you have processes in place to remedy the causes of it so that it doesn't happen again.

Cause of serious privacy breaches
(since 1 December 2020)



Case study : Inappropriate access to personal information

In October 2021, media revealed that a group of ACC call centre workers had a private Snapchat group, sharing images of details of people's injuries. One of the screenshots contained information which would identify a client.

While ACC acted immediately to notify the affected individual and rectify the situation, these types of breaches cause further harm to people who were already in a vulnerable position and risk making other people less willing to seek help when they need it.

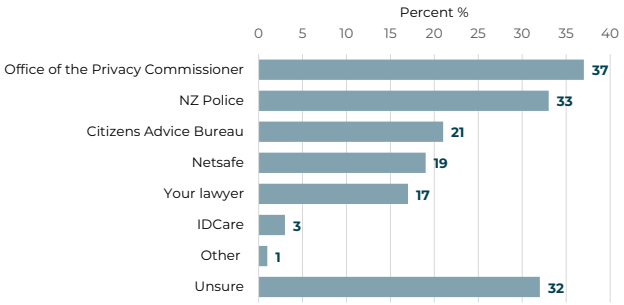
Recognising the importance of effective privacy and information management to trust and confidence in ACC, the ACC Board commissioned an independent review into the access and use of client information in November 2021.

Insight 4

OPC is here to help agencies and individuals when something has gone wrong

Over a third of respondents identified the Office of the Privacy Commissioner as the right organisation to contact if they were affected by a privacy breach, with Police a close second. However, three in ten New Zealanders did not know where to turn to for help should they be the victim of a privacy breach. This shows there is still work to do in raising awareness of where to turn for help, both for individuals and agencies.

Q: Which organisation would you contact in the event of a privacy breach?
(AKR Survey)



*Note: The figures add up to a number greater than 100% because more than one answer was possible.

In the past year, seven percent of survey respondents said they had experienced a privacy breach. Four in ten of those affected by a breach said that they had contacted OPC in relation to their concern. Of those who didn't report to us, the principal reasons were that they didn't feel it was important enough, or that they dealt with it direct with the organisation or agency involved.

Our focus is on resolving disputes and where appropriate we will try to facilitate the settlement of a complaint. Most settlements are apologies or a release of information, although financial compensation may be involved. Most investigations are resolved within six months but occasionally they take longer depending on the individual circumstances.

If someone does make a complaint to us, our first step will be to ensure that they have tried to resolve the issue with the agency involved. Most businesses and organisations will want to help resolve issues quickly. However, that is not always successful, and this is where OPC can step in.

During the year to 31 March 2022, OPC received:

363 Complaints

234 Serious breach notifications

4244 Inhouse enquiries

4241 Call centre enquiries

Sometimes we will also look into an issue where no-one has made a complaint if we think it is systemic in nature or that there is a power imbalance between the individual and agency which means that people are unlikely to complain to us or the agency.

While some agencies are quick to report privacy breaches, the majority continue to be slow with fewer than half reported within our expected three days.

Timely reporting enables us to provide the best advice about minimising the risk of harm to those who have been affected. Timely reporting also keeps you on the right side of the law. It is a criminal offence not to notify us of a breach that has or is likely to cause serious harm. We have been clear that our expectation is that this should be done within 72 hours of becoming aware of the breach.

Case study: Managing an intentional and malicious breach

In May 2021, Waikato District Health Board was hit by a major ransomware attack that impacted systems and services, causing delays to some medical care and support for vulnerable New Zealanders. During this attack hackers stole the personal information relating to a number of patients and staff, sending some data to New Zealand media as 'proof' of the attack. Months later the personal details of these individuals were disclosed onto the dark web.

The DHB notified us within hours of becoming aware of the attack. This enabled us to work alongside them, acting as a sounding board as they navigated their way through the many complex privacy implications of this significant attack including assessing how to approach the notification and support of affected individuals and communicate an evolving and uncertain situation to the public.

Sources used for this report:

- AK Research for the Office of the Privacy Commissioner, *Privacy concerns and sharing data*, 2022

  Full survey results and methodology can be found here:

https://privacy.org.nz/assets/New-order/Resources-/Publications/Insights-reports/AK-Research-and-OPC-Privacy-concerns-and-sharing-data-April-2022.pdf

- UMR Research for the Office of the Privacy Commissioner, *Privacy concerns and sharing data*, 2020
- Colmar Brunton for InternetNZ, *New Zealand's Internet insights*, 2021

https://internetnz.nz/assets/Uploads/Internet-insights-2021.pdf

- Operational data, derived from OPC sources

About the data:

- All OPC operational data refers to period 1 April 2021 - 31 March 2022, unless otherwise stated

Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner I Te Mana Mātāpono Matatapu
PO Box 10094, The Terrace, Wellington 6143
T +64 4 474 7590 Fax +64 4 474 7595
E enquiries@privacy.org.nz
www.privacy.org.nz