Seeing the forest *and* the trees: using de-identification effectively to protect privacy

Natasha Mazey, Marcin Betkier, Reuel Baptista, Sophie Watson

Executive summary

Organisations that process personal information increasingly rely upon de-identification to protect privacy as a tool to comply with the regulations, and as a privacy-preserving safeguard. But, achieving robust de-identification can be a complex matter and many New Zealand organisations, especially the smaller ones, lack the resources to provide de-identification expertise. They need leadership and guidance, and greater awareness of de-identification issues.

But, despite global trends, New Zealand authorities and public agencies have remained silent to provide such guidance about what de-identification means domestically. They do not effectively communicate good practices and do not further publicly debate on privacy risks. With the proliferation of the use of personal information in many ongoing projects, such as the Consumer Data Right or proposed health information platform (Hira), this space needs to be addressed very soon.

If not appropriately considered in the early stages of information technology projects, de-identification can either hamstring those projects or undermine their effectiveness entirely. On the contrary, if applied correctly, de-identification techniques should impact architectural design and enable future opportunities. This should be acknowledged in Privacy Impact Assessments.

We provide recommendations to mature the understanding and practice of de-identification domestically. In this respect, we describe below in detail the purpose and scope of the identification guidelines and discuss how they can be implemented in New Zealand.

Introduction

In our commentary *The Ignorance of Anonymisation to Protect Privacy*[1], published in September 2020, we explained how the terms "anonymisation" and "de-identification", although often used inter-changeably, are different. "De-identification" is ambiguous; "Anonymisation" is not. De-identification is the use of techniques to decrease the risk of identifiability of individuals. Anonymisation is a result of an irreversible process that will reliably prevent re-identification with certainty. Anonymisation is not always possible to attain but may also not be necessary or not needed to protect privacy. Both are highly dependent on context and risks that may be posed by data themselves, technology, people, processes, associated data, and the changes of any of these over time.

De-identification and anonymisation are moving targets. "De-identification" represents a broad, varied spectrum of privacy protections and should not be taken at face-value as being effective without further

[1] The Ignorance of Anonymization to Protect Privacy; https://www.privacyfoundation.nz/wp-content/uploads/2020/09/The-Ignorance-of-Anonymisation-to-Protect-Privacy.pdf dated September 2020.

information as to what type of risk the data may be exposed to in a specific instance. We also noted various risk factors that may call for stronger or weaker de-identification techniques or processes for either effective de-identification or anonymisation.

In this commentary, we go further with that thinking and consider our progress in maturing our understanding and use of de-identification and anonymisation. We explain why it is even more important and timely to focus now on de-identification and show how we can advance that in New Zealand.

Unless we specifically mean "anonymisation", we use the term "de-identification" to include both de-identification and its perfect, sometimes unattainable goal, anonymisation.

Progress in identifying and responding to de-identification risks

De-identification is a hot topic within privacy and data protection circles. Recent discussion around de-identification and anonymisation shows a broadness of views relating to it, but also a converging path to achieving practical outcomes. De-identification is commonly accepted as one of the practices of "Privacy By Design" and, more recently, referenced as a form of "Privacy Enhancing Technology"[2], although we expect the latter term to be a little misleading by overlooking its simpler purposes and applications.

Early debate and more conservative views were that anonymisation or meaningful de-identification is not possible at all. Paul Ohm, in his seminal article about the failure of anonymisation, put forward the idea of a spectrum between directly attributable information and information that is anonymous,[3] which was later called 'the spectrum of identifiability'[4] (also presented in our previous commentary). He presented a view that anonymisation is not attainable and anonymous data is not necessarily useful[5]. Consequently, additional regulations and obligations on the data owners should be imposed to preserve privacy interests.[6] Gone are the days when the removal of direct identifiers, like name, date of birth or social identifier (for example, IRD or driver's licence) were considered to create anonymous data.

Agencies and researchers have since further explored de-identification and anonymisation failures, developing and adopting risk-based approaches. They suggest the use of process-based approaches to protect against re-identification[7] and to account for the relationships between data and data environment.[8] This asks the owners of data to perform a holistic exercise to consider re-identification risks and respond to them from various perspectives.

Following that, in more recent public discourse prompted by COVID-19 concerns, improvements and opportunities relating to de-identification practices came to the forefront as the world collected and shared COVID-19 data for contact tracing, border control, public health management and research. Within New Zealand, concerns were raised about the publicity of "anonymised" detail of positive COVID-19 cases' close contacts and location history, which led to the identification, public scrutiny and harassment of individuals with COVID-19.[9] There was also significant public debate with regards to the

---

[2] Omar Ali Fdal, July 2022 : What are privacy enhancing technologies (PETs) and how can you choose the right one(s); https://www.cpomagazine.com/data-privacy/what-are-privacy-enhancing-technologies-pets-and-how-you-can-choose-the-right-ones.

[3] Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA Law Review 1701 at 1749.

[4] Chapter 2: How do we ensure anonymisation is effective? in "ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance" (7 March 2022) <https://ico.org.uk> at 7–8.

[5] Ohm, above n 3, at 1752.

[6] At 1760 ff.

[7] Ira S Rubinstein and Woodrow Hartzog "Anonymization and Risk" (2016) 91 Washington Law Review 703 at 729 ff.

[8] Mark Elliot and others "Functional anonymisation: Personal data and the data environment" (2018) 34 Computer Law & Security Review 204 at 212–3.

[9] Anusha Bradley "Covid-19 patients suffered harassment and abuse" (17 October 2020) RNZ <www.rnz.co.nz>.

2021 *Whānau Ora Commissioning Agency* court case concerning the release of data to enable the identification of non-vaccinated Māori.[10] In that case, the release of data was deemed necessary for the goals of public health.

But, the questions about appropriate practices of individuals' data, and effective de-identification had begun to emerge prior to the COVID-19 pandemic. There were a number of political and voting scandals in the US, Canada and the UK (for example, Cambridge Analytica of 2018 and Clearview AI of 2020) prompting inquiries and public debate. Some regulators were proactively trying to clarify what de-identification should mean in our complex digital and information environment.

As a result of those developments, we have increasingly more legal guidance about what robust techniques could look like, and what pitfalls and assumptions need to be accounted for to align with the intention of the law and the outcome individuals would commonly expect from the words' de-identification' and 'anonymisation'. Countries who lead the charge on this include Australia,[11] the US,[12] European Union,[13] and the UK.[14] Increasing new leadership is also being provided from likes of Singapore[15] and Korea[16].

Despite those global changes and progress, the New Zealand government authorities and regulators have so far remained silent on these issues. They seem to rely on the report and practices of Stats NZ which treat privacy as an aspect of confidentiality.[17] We believe it is important that New Zealand issues clear guidelines and expectations with regards to appropriate de-identification under local privacy legislation. A robust de-identification framework for data could provide our economy with more certainty as to the safe, lawful use of personal information while enabling the pursuit of public and business objectives such as research and development, which rely on de-identification as privacy-preserving safeguard. This is especially urgent in light of various new government public initiatives.

Current initiatives that need certainty around 'de-identification'

The New Zealand government has a number of current and emerging initiatives concerning the greater collection, access and use of personal information. A number of these initiatives, and the potential to fully take advantage of these changes while mitigating their accompanying privacy threats, rely on de-identification as a key, foundational privacy and confidentiality preserving measure.

---

[10] Office of the Privacy Commissioner "Case note [2022] NZPrivCmr 1: Te Pou Matakana Limited v Attorney-General judicial review: Privacy Commissioner's intervention (No 1) [2021] NZHC 2942 and (No 2) [2021] NZHC 3319" (28 January 2022) <www.privacy.org.nz>; *Te Pou Matakana Ltd v Attorney-General I* [2021] NZHC 2942; *Te Pou Matakana Ltd v Attorney-General II* [2021] NZHC 3319.

[11] Christine M O'Keefe and others "The De-Identification Decision-Making Framework" [2017] Office of the Australian Information Commissioner 93; eHealth Queensland *De-identification and anonymisation of data guideline* (State of Queensland (Queensland Health), 2021).

[12] E.g. Simson L Garfinkel *De-identification of personal information* (NIST IR 8053 National Institute of Standards and Technology 2015); Future of Privacy Forum "Visual Guide to Practical Data De-identification" <https://fpf.org>.

[13] Different national guidance mainly basing on Article 29 Working Party *Opinion 05/2014 on Anonymisation Techniques* (0829/14/EN WP216 2014). Also, new guidance is being prepared by the European Data Protection Board.

[14] Currently consulted new guidance, see "ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance", above n 3.

[15] Singapore's PDPC Guide to Basic Anonymisation; https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.ashx released 31 March 2022.

[16] Korea's PIPC press release for Revised Guidelines for Handling Pseudonymous Information; https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7616 released 21 October 2021.

[17] StatsNZ *Data Confidentiality Principles and Methods Report* (2018).

Current initiatives include:

- Hira (proposed new national health information platform)[18]
- Aotearoa Immunisation Register[19]
- Consumer Data Right[20]
- Access to the data held by Statistics NZ for research purposes (see s 51 of the Data and Statistics Act 2022)
- Biometrics Code of Practice [21]

We believe all these initiatives need to rely on robust de-identification practices to support individuals' privacy interests.

Current guidelines and indicators of expected practice

The only guidance which is available and may be used as an indicator of practice so far is *Principles For The Safe And Effective Use Of Data And Analytic*[22] issued by Stats NZ in collaboration with the Privacy Commissioner in May 2018. This describes six high-level principles that is recommended to guide data and analytics decisions, but like the Information Privacy Principles these are broad principles only. We do not expect these are enough to support agencies to effectively address privacy concerns or to practically deliver these, particularly if these may be contextually driven.

Stats NZ has provided additional reports on their 'confidentiality' methods relating to census data which include de-identification practices (such as *Applying Confidentiality Rules to 2018 Census Data and Summary of Changes since 2013 [23]).* While these reports could serve as guidance which others could adopt, we note the Confidentiality Rules, and associated practices and policy objectives, described within the reports are intended for Stats NZ use only, and it is unclear how expectations could or should change in other contexts. The primary purpose and scope of these reports seems to support their accountability obligations and transparency commitments to the New Zealand public. In other words, the information provided is not anticipated or intended to act as guidance for other agencies. It is unclear if the examples these reports provide are fit-for-purpose for other agencies in the protection of privacy or to comply with the Privacy Act 2020.

Data.govt.nz (in partnership with the Department of Internal Affairs) also provides some guidance in the *Data Confidentiality Principles and Methods Report* which is publicly available. However, this is also targeted in its application and intended audience. We expect information included in this guidance could be leveraged to support more mature data practices across New Zealand and could be communicated as such.

The need and benefit of a de-identification standard also spans to the private sector. Some initiatives (such as the Consumer Data Right) will be directly applicable in the private sector. Other sectors would also benefit from further clarity and update to expected acceptable practices. For example, this may include sectors governed by clinical or research ethics obligations for academic and scientific purposes. We would suggest any de-identification standard considers and draws upon existing industry codes or

[18] Ministry of Health NZ "Hira – connecting health information – Te Whatu Ora" <www.tewhatuora.govt.nz>.
[19] Ministry of Health NZ "https://www.tewhatuora.govt.nz/our-health-system/digital-health/the-aotearoa-immunisation-register-air-2/the-aotearoa-immunisation-register-air/" Ministry of Health NZ <www.tewhatuora.govt.nz>.
[20] Ministry of Business, Innovation & Employment "Consumer data right" <www.mbie.govt.nz>.
[21] "Privacy Commissioner to explore biometrics code" <https://www.privacy.org.nz/publications/statements-media-releases/privacy-commissioner-to-explore-biometrics-code/
[22] Stats NZ, May 2018 <https://www.stats.govt.nz/assets/Uploads/Data-leadership-fact-sheets/Principles-safe-and-effective-data-and-analytics-May-2018.pdf>
[23] Stats NZ, Sept 2019 <https://www.stats.govt.nz/methods/applying-confidentiality-rules-to-2018-census-data-and-summary-of-changes-since-2013>

standards that may specific de-identification or confidentiality obligations already. Future standards or guidelines should also highlight the impact of the varying contexts, needs and privacy concerns of its intended application so that de-identification activities effectively support compliance with their privacy obligations.

The management and re-opening of the COVID-19 pandemic economy to tackle the global economic slowdown created obligations on agencies to support the management of COVID-19 transmission. It was made clear that the Privacy Act 2020 needed to be prioritised in these efforts; necessity and data minimisation principles were the main targets. But, the broadness of the Informational Privacy Principles leaves ambiguity in their application. Agencies would have benefited from further certainty and confidence as to the permitted limits of the use of personal information to support administration and stimulate economic growth and activity, rather than constrain or delay activity. Further certainty would have provided confidence to identify when compliance may be achieved. It may have provided more confidence to promote greater transparency of data practices. Instead, agencies were left guessing, and some may have opted for more conservative practices, which may have hindered business activity or the next steps of recovery from the pandemic. We expect clearer de-identification guidance would continue to support economic activity in the future, especially in the context of research and development, data analytics and new technologies.

De-identification is not a magic, silver bullet

We are pleased to see government and public sector agencies performing more privacy risk analysis, usually in the form of Privacy Impact Assessments. However, we are concerned about the ambiguous references to rely on de-identification without further consideration and planning at the outset.[24] De-identification is not a magic, silver bullet. It does not allow a free pass to collect, use and share personal information unchecked. It involves a balanced threat to privacy and a risk to individual and individuals' collective rights and freedoms. It demands a measure of re-identification risk and that the risk is dealt with appropriately.

Approaches to de-identification can vary widely and if not appropriately considered in the early stages of information technology projects, can either hamstring those projects or undermine the effectiveness of de-identification entirely. That is because de-identification methods underpin and inform data collection requirements and information system management designs. These decisions can have a significant effect on how architectural solutions shape up and work practically. If done right, it is reasonable to expect that certain de-identification decisions will prohibit future uses by the very design of the solutions and remove flexibility for some changes. Considering the number and nature of public initiatives that intend to, or could, leverage de-identification, providing clarification now will likely save the tax-payer and investors down the road, while also better enabling the digital industry to get it right and supporting growth opportunities.

The re-identification risk analysis analogical to the one in Privacy Impact Assessments should reflect de-identification trade-offs. The approach for de-identification does not always need to be finalised in full early on, but key decisions and trade-offs that will shape the architecture of data, technology and processes should be identified early. With regards to public initiatives, further transparency regarding the approach or limitations introduced by de-identification is needed for transparency, accountability, and the social licence they are aspiring towards. This is because that will enable the public to debate, feedback and improvement according to stakeholders' interests.

[24] For example, '[*n*]*on identifiable (or de-identified) information may be used for purposes related to the public health response to COVID-19 (which may include planning for future potential events or research)'.* See the Ministry of Health's Contact Tracing App - Privacy Impact Assessment: https://www.health.govt.nz/system/files/documents/pages/contact_tracing_app_pia_final_20201204.pdf.

The law about de-identification

Those most effectively placed to manage data, and more specifically, the management of personal information and privacy interests, are the agencies responsible for its collection and use. This is aligned with the Privacy Act 2020, which sets a principles-based approach for agencies to interpret and apply the law accordingly. There is a strength in this approach, as it offers flexibility to promote the right outcomes being met in the most efficient way.

The Privacy Act 2020 contains certain references to de-identification that may be used by agencies holding personal information. That is because it contains exceptions whereby those agencies do not need to comply with certain Information Privacy Principles (IPP 2, IPP 3, IPP 10 and IPP 11) if they believe that the information will not be used in a *form* in which the individual concerned is identified. That suggests that information, which is in a form where the individual cannot be identified, is still 'personal information' as the Information Privacy Principles only apply to personal information. So, although the concept of *'form'* is not further defined in the Privacy Act 2020, it could be interpreted to mean information that has had certain methods of de-identification or anonymisation applied in order to make sure the individual cannot be identified. But, it is not as clear as, for example, the Australian Privacy Act 1988 (Cth) that provides for the definition of "de-identified" personal information.

Therefore, in the case of de-identification, we argue that more explicit guidance and clear boundaries need to be set forth for agencies to work within and to reduce ambiguity and confusion. A clear starting point would be to build off the concepts behind the exception that the Privacy Act 2020 already has in place.

Resource shortage

Privacy and data protection specialists are few and far between in New Zealand. They are often specialists in a number of areas relating to privacy and personal information – the law, technologies, data governance, identity management, data breach management, complaint resolution and supplier management. Not surprisingly then, that larger organisations have skilled privacy professionals on-hand that go beyond the designated, well-meaning Privacy Officer who fulfils the obligations set forth in the Privacy Act 2020. De-identification is yet another tool to be curated for their toolbox, and many are left to look overseas for guidance and to import and translate these for New Zealand settings. The reality is that many local privacy professionals may combine and coordinate this varying expertise, but they rely heavily on other resources to be able to perform their role sufficiently. In the case of de-identification, technical expertise is often needed from cybersecurity, data governance, data analytics and enterprise systems and infrastructure professionals.

Many agencies in New Zealand are 'Small and Medium Enterprises' (SMEs) that do not have the resource available to provide privacy, let alone de-identification, expertise. This may include community groups and charities. They may outsource legal work to law specialists and various data, information, or systems work to other specialists. There is a gap for this type of expertise and SMEs and these service providers need proactive support. It is not fair or reasonable to expect these agencies to provide adequate, future-proofed de-identification protections and solutions when the best resources are likely engaged by bigger companies. Those smaller agencies are particularly in need of de-identification guidelines.

What should be covered by the guidelines

De-identification guidelines need to be practical. It may be difficult, and perhaps inappropriate, to prescribe specific methods and techniques on the assumption that these may apply on a "one-size-fits-all" basis. Any methods and techniques will likely be applied depending on the context and will balance a range of considerations, including probable privacy threats. Ultimately, the appropriateness of any de-identification method will be a reflection of its particular case and its context. Having said that, it is possible to discuss some of those factors in general. De-identification guidelines,

and any decisions relating to the appropriateness and risk of de-identification methods, should reflect the following factors.

i. *Potentially identifying information (on its own or in combination)*
    1. Removal, suppression, or segregation of all unique identifiers (including a definition of what this should include at minimum).
    2. Removal, suppression, or segregation of all quasi-identifiers, which may in combination be identifiable features (including a definition of what this should include at minimum).

ii. *Singling out or inferring other information*
    1. Sensitivity and uses for data, and the potential for drawing inferences.
    2. Probability to identify by random selection and singling out.
    3. Data matching and linkability risks; between and within datasets that might be available to a person who would attempt to re-identify the data.

iii. *Nature of information over time*
    1. Sensitivity and accuracy of data over time.
    2. Whether data may change and ease to update (for example, biometric data cannot change, but political preferences may)
    3. Classification of "de-identified" vs "anonymous", the level of risk and what may be appropriate safeguards are time bound and may change over time. This may be because new datasets may be available for matching or new systems, tools or data are introduced.
    4. The level of re-identification risk over time, including:
        1. Current data and technical landscape, which an agency has control over.
        2. Reasonably likely and foreseeable data and technical landscape, which an agency may have control over in the future (for example, intentions to expand data collection and analytic capability).
    5. Likelihood to re-identify the information.
    6. Technical and organisation controls which prevent unauthorised or inadvertent access, use or disclosure to reduce the likelihood of re-identification.
    7. Appropriate methods for de-identification which consider the nature and context of information and whether methods may be appropriate to achieve "anonymisation".
    8. "Anonymous" data must be considered to have a reasonably current and irreversible process to prevent re-identification.
    9. Relevant subject matter experts that could reasonably support expert determination, for example, data subject matter experts, data analytic specialists, enterprise system or infrastructure specialists, cybersecurity specialists, AI specialists (if applicable), and statistics specialists.
    10. To tackle those risks, 'threat models', which reflect uses case for re-identification threats, should be considered and used to inform decision making.

iv. *Cultural and social considerations*
    1. Last but not least, cultural values, principles and considerations may be relevant and should be considered in the application of de-identification. This should have regard to New Zealand’s indigenous communities and other diverse multi-ethnic populations (e.g. Māori, Pacifica, Asian ethnic groups), as well as other minority groups who may be especially vulnerable to re-identification, singling out or unfair discrimination or other risks in certain scenarios (e.g. religious, victims, refugees, migrants).

To tackle the privacy risks, a 'threat model' which reflects use cases for re-identification threats should be considered and used to inform decision making. Those threats may reflect particular characteristics of a potential 'attacker'. That could be a layperson, a motivated intruder, a specialist in the field, a government agency, or an own employee who is negligent or accidentally makes a mistake.

Methods of de-identification

De-identification does not need to be especially difficult. There are methods that are more statistically or mathematically based, which may be useful (for example, K-anonymity, L-diversity, T-closeness, and differential privacy). They demand expertise and care in ensuring the appropriateness over time for its application. But, there are also simpler examples that can be implemented without significant special knowledge, which include:

- Removing direct and quasi-identifying data
- Pseudonymisation
- Scrambling
- Randomisation
- Aggregation and generalisation
- Suppression
- Masking
- Encryption and hashing
- Adding "noise"
- Database segregation

How to adopt the de-identification guidelines in New Zealand

We note that de-identification or anonymisation standards that exist globally are usually found in statutory law. For example, the European General Data Protection Regulation (GDPR) states in (non-binding) recital 26 *"(…) account should be taken of all the means reasonably likely to be used to identify the person directly or indirectly*" including "*all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".* As discussed above, the New Zealand law is not that detailed as a limited reference to de-identification may only be found in the exceptions to Information Privacy Principles 2, 3, 10 and 11 so it cannot provide direct guidance for the regulator or an agency using personal information.

Having said that, the case law may fill in that gap. It is well established there, that identifiability *"can be made on the basis of a link identifying the individual, whether that link is obtained from the recipient's own knowledge or by other means"*.[25] Also, notably, the New Zealand Human Rights Review Tribunal demonstrated its readiness to draw standards from the GDPR,[26] so it would be possible to use the European law more directly, as a wider global standard which New Zealand seeks to be compliant with by providing an "adequate level of protection". Ultimately, the harmonisation of the regulations across the borders is a very important factor for the international businesses.

All of this may provide some direction as to domestic expectations for those already familiar with EU requirements and where the Human Rights Review Tribunal may have jurisdiction, but further awareness and understanding of what this means for other businesses or how these factors into government agency activity are unclear.

Against this backdrop, we recommend:

- **An independent, multi-disciplinary advisory body to provide specialist guidance and public oversight.**
  This should reflect current and future technologies, information systems, data governance and security trends. This body could independently assure public sector initiatives using de-identification and monitor public sector datasets for enterprise/national privacy risks. We suggest this could be the Office of the Privacy Commissioner if resourced sufficiently.
- **Practical guidance about the scope and implementation of de-identification.**

[25] *Proceedings Commissioner v Commissioner of Police* [2000] NZAR 277 (CRT) at 285.
[26] See *Naidu v Royal Australasian College of Surgeons* [2018] NZHRRT 23 at [41] – [43].

Guidance should be provided for different sectors, for example, healthcare sectors, financial sectors and children-related sectors. This should practically reflect the varied nature of New Zealand agencies and the availability of privacy expertise. We recommend guidance be clear on key outcomes and assumptions that must be met; and, where applicable, clear metrics or KPIs that can support reliable outcomes being achieved.

More specifically, we suggest:

- **Government agencies provide transparency about their own de-identification frameworks** to inform a common understanding of acceptable practice within New Zealand, which other agencies could learn from, and support ongoing discussion and advancement of this topic.
- **Setting de-identification standards for different industries**
  For the private sector, for example, standards could include a "motivated intruder test". This test, which is found in UK data protection case law, assesses risks within the bounds of a relatively inexpert member of the public, and someone with access to significant specialist expertise, analytical power or prior knowledge.[27] In short, it considers possibilities where someone is reasonably competent, has access to resources and likely knows some investigative techniques, but starts without prior or specialist knowledge of data, access to specialist equipment and does not need to resort to significant criminal acts. [28] That standard would set the high, but not unattainable threshold and could be a good starting point to ground domestic de-identification standards.
- **De-identification of Personal Information Guidance or Standard**, or other codes of practice, be enacted. This could be regulated through the Privacy Act 2020 and sit alongside the likes of the Health Information Privacy Code 2020.

Conclusion

We realise that navigating de-identification can be tricky. By definition, the term "de-identification" still involves an inherent risk of re-identification. Even the best approach is likely vulnerable to being unravelled by a skilled, persistent expert with access to resources. But, operationalising de-identification and implementing good, risk-based organisational and technical practices is possible without difficult or specialist resources or techniques. We should not shy away from demystifying de-identification and establishing good practice expectations. This could help with building trust in the public sector and help the New Zealand digital sector to operate efficiently on global markets.

It may be easier to shroud de-identification in mystique and leave it to be a discretionary effort of certain, varied experts. This may be effective in other areas, but given the multi-disciplinary expertise needed, we argue this approach is not sufficient. We can look to overseas to help get us started, but we need further guidance and leadership within New Zealand. De-identification is a moving target, and support is needed for New Zealand agencies.

[27] Chapter 2: How do we ensure anonymisation is effective? in “ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance”, above n 3, at 15 ff.
[28] Chapter 2: How do we ensure anonymisation is effective? in At 15–16.