Regulatory Impact Statement

Additional decisions for the Privacy Bill

Agency Disclosure Statement

1. This Regulatory Impact Statement has been prepared by the Ministry of Justice.

2. The options presented in this paper relate to previous decisions by Cabinet to reform the Privacy Act (the Act) to send strong signals about the importance of privacy of personal information.

    - The first part of the paper responds to the recommendations of the Data Futures Forum (DFF)[1] concerning the mitigation of privacy harms that can be caused by the release of de-identified data, and a direction by Cabinet for the Privacy reforms to respond to that recommendation.

    - The second part amends previous Cabinet decisions to ensure the policy intent of those decisions is achieved. The relevant decisions relate to the details of the supporting framework for mandatory data breach notifications, and the power to issue compliance notices for breaches of the Act. Policy design relating to these areas is restricted by the direction and intent of previous Cabinet decisions.

Part I re-identification of de-identified personal information

3. Decisions to address risks associated with the release of de-identified information have been informed by previous Cabinet decisions. Based on advice provided by DFF, Cabinet directed Justice to consider DFF recommendations in current privacy reform processes. There is limited evidence about the extent of problems associated with de-identified data in New Zealand, however, and we have had to rely on overseas examples about the potential harm that can be caused. Considering both the commercial and other benefits that de-identified data can generate and the progress of the Open Government Data programme, however, we have assumed that such trends will eventuate in New Zealand.

Part II mandatory breach notifications

4. Analysis of options amending previous Cabinet decisions has been constrained by lack of empirical evidence about the direct and indirect economic costs and benefits of privacy law settings to individuals, businesses and Government. As with analysis supporting original Cabinet decisions, the current regime of voluntary reporting of data breaches constrains the lack of data on the scale and nature of privacy breaches.

[1] The Data Futures Forum was an independent advisory group appointed by the Ministers of Finance and Statistics to give advice on how data can be safely used to grow a prosperous and inclusive society. The Forum published a set of recommendations in July 2014.

5. We have been unable to estimate the costs and benefits of policy design options and, therefore, we have largely provided judgements about the order in magnitude of different types of costs for agencies, individuals and the Office of the Privacy Commissioner. Judgements we have made about the impacts on agencies are included in relevant sections, and have been undertaken in close consultation with the Office of the Privacy Commissioner (OPC).

Chris Hubscher
General Manager
Electoral and Constitutional
Ministry of Justice

Date 4 February 2016

Executive Summary

6. In 2014 Cabinet agreed to the drafting of a new Privacy Bill (the Bill) that responded to the Law Commission's review of the Privacy Act 1993 (the Act), and to modernising the Act [CAB Min (14) 10/5A]. During the drafting of the Bill some policy design issues have arisen and this RIS analyses options to address those issues.

Part 1: re-identification of de-identified personal information

7. With respect to the emerging potential for people's personal information to be re-identified from de-identified datasets, the preferred option is to:

   a. the Office of the Privacy Commissioner (OPC) develop guidance to support good de-identification practices

   b. a new information privacy principle (IPP) be introduced, to discourage agencies from taking deliberate steps to re-identify and not act on inadvertently re-identified data. The wording of this IPP, and relevant exceptions, will be finalised during the drafting process in consultation with relevant agencies.

8. De-identified information refers to personal information from which some personal identifying information has been removed so that the information does not directly or easily identify an individual. As information which has been effectively de-identified does not meet the definition of personal information[2], the Act does not contain provisions relating to its use. However, re-identification of de-identified data can occur easily, through both inadvertent and deliberate means, and result in privacy harm. There is real commercial incentive to deliberately undertake such re-identification.

9. Clarifying limits for use of re-identified information will enable New Zealand agencies (both public and private sector) and given them confidence to make better use of datasets and share more de-identified information with others. The proposals, if agreed, will introduce small compliance costs for agencies as they will need to ensure that they comply with the requirements and limitations as expressed in guidance and the new privacy principle. These costs can be offset by the benefits of the new requirements: protecting individuals from this emerging privacy risk will mitigate the reputational issues for the agencies concerned and contribute to increased trust and confidence in the data sharing environment.

[2] Personal information is information about an identifiable individual. De-identified information is personal information that is somewhere on a spectrum between entirely anonymous (e.g. a statement of the current New Zealand population) to easily re-identifiable (e.g. a drivers licence with the last name blacked out). The Privacy Act definition of personal information has some difficulty precisely delineating this spectrum because within any de-identified data set will be some number of individuals that can easily be re-identifiable.

Part II: mandatory breach notifications

10. The other options in this paper relate to further clarification around aspects of mandatory breach notification policy design, and these are aligned with the direction of previous Cabinet decisions to further reinforce the package of privacy reforms signalling the importance of people being confident that their personal information will be kept private by the agencies that hold it.

11. These amendments will, overall, reduce compliance costs, while improving the protections afforded to individuals. They will make legislative provisions easier to work with for agencies, while ensuring they can be held accountable in specific, and appropriate, circumstances.

Background

12. The Act establishes New Zealand's information privacy framework. It regulates what can be done with information about individuals and has wide-reaching implications – it applies to every 'agency', including Government, private sector businesses, and voluntary sector and non-Government organisations.

13. There are two key features of the Act. First, the Act generally requires agencies to handle personal information in accordance with 12 information privacy principles (IPPs). The IPPs govern personal information at all points of its lifecycle, from its collection to destruction. The IPPs are intended to be flexible enough to enable agencies to develop their own information-handling policies, tailored to the needs of the agency and its users or customers. They can be overridden by any other enactment.

14. Second, there is a right to complain to the Commissioner and ultimately to the Human Rights Review Tribunal. If a breach of the IPPs results in harm occurring to individuals, the Tribunal may make orders and award damages. Under the Act the Commissioner has an important role to play in resolving complaints as well as educating agencies about their responsibilities and providing guidance in how to meet them.

15. From 2006 – 2011 the Law Commission reviewed the law relating to privacy, and issued a number of reports. In April 2014 Cabinet agreed to the contents of a Privacy Bill that embodied the majority of the Law Commission recommendations [CAB Min (14) 10/5A]. The key proposals create stronger incentives for agencies to identify and prevent privacy risks, and give the Privacy Commissioner (the Commissioner) a stronger regulatory role in responding to privacy breaches.

16. A regulatory impact statement (RIS) was prepared to accompany the 2014 Cabinet paper in order to support Cabinet's decision making.

17. Subsequent to that decision-making, Cabinet agreed that a recommendation from the DFF about the regulation of re-identification of de-identified personal

information be considered as part of the reform of privacy settings [EGI Min (15) ½ refers].[3]

18. During the drafting of the Privacy Bill that responds to Cabinet's decisions, additional policy design issues have arisen which require further decisions from Cabinet.

19. This RIS is presented in two parts:

    19.1. PART 1 relates to the DFF's recommendations about re-identification of de-identified personal information

    19.2. PART II relates to Cabinet's decisions about mandatory breach notifications.

Status quo

Part I: Re-identification of de-identified personal information

20. The Act currently:

    20.1. requires agencies that hold personal information to ensure the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:

    - loss; and
    - access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
    - other misuse.

    While not explicit, 'other misuse' could encompass consideration of the potential for de-identified information being re-identified.

    20.2. does not provide appropriate limitations on agencies that may seek to re-identify de-identified personal information. Although the re-identified information will be subject to the privacy principles, it could be "repurposed" in ways unexpected by the individuals concerned.

Part II: Mandatory breach notifications

21. Currently, the Commissioner only becomes aware of privacy breaches (also known as data breaches) through voluntary notification, complaints and media reports, resulting in inconsistent practices. This approach does not enable early

[3] The Law Commission, in its review of the Privacy Act (2011), made no recommendations relating to de-identified data, as this review predated the work of the DFF. It did, however, note that advances in technology have made it easier to re-identify information that has been anonymised or de-identified, and that this may have implications for the concept of "identifiability" in future.

identification of, and response to, the serious harm that can result from a privacy breach. Nor does it provide the Commissioner with a system-wide view in order to improve privacy practices.

22. In 2014 Cabinet approved a two-tier notification regime for privacy breaches to enable the Commissioner to become aware of, and begin to address, emerging or systemic privacy issues. The two tiers are:

    22.1. Material breaches – agencies are required to take reasonable steps to notify the Commissioner of any material breaches, taking into account: the sensitivity of the information; and number of people involved; and indications that the breach was caused by a systemic problem.

    22.2. Serious breaches – agencies are required to take reasonable steps to notify the Commissioner and affected individuals where there is a real risk of harm, unless an exception applies.[4]

23. Cabinet agreed to a $10,000 financial penalty for agencies that fail to notify the Commissioner of either a material or serious breach. This is considered to provide an effective incentive to ensure breaches are notified to the Commissioner, thus allowing the Commissioner to become aware of, and begin to address, emerging or systemic privacy issues. Currently, there is no remedy for affected individuals who are not notified by agencies of a serious breach.

Objectives and evaluation criteria

24. The proposals considered in this RIS about privacy settings should be consistent with the objectives of the original Cabinet decisions relating to current privacy reforms. Those objectives were sound, balanced, law that ensures:

    (a) individuals have confidence that information shared with private and public sector agencies will be adequately protected

    (b) public and private sector agencies are able to access the information they need from the public to provide goods and services as effectively and efficiently as possible.

25. These objectives can sometimes be in tension with each other. The ability of agencies to access personal information to provide goods and services, if not adequately regulated, can undermine the confidence individuals have that their personal information is being adequately protected. While an appropriate course of action may depend on the relative weighting given to each of these objectives when in tension with each other, it is the Ministry's position that objective (a) is prior to objective (b). If objective (a) is not met, individuals will be less willing to share their personal information, ultimately reducing the ability of agencies to

[4] The exceptions, as currently stated, are to "protect trade secrets, security, and vulnerable individuals".

achieve objective (b) by accessing personal information necessary to the provision of goods and services.

26. Since the setting of those objectives the DFF has developed four principles to guide the use of data. While only the issue of re-identified information responds directly to DFF recommendations, these principles apply to all data use, and so are also valid to all options considered here. They are:

    - **Value:** NZ should use data to drive economic and social value and create a competitive advantage
    - **Inclusion:** all parts of NZ society should have the opportunity to benefit from data use
    - **Trust:** data management in New Zealand should build trust and confidence in our institutions
    - **Control:** Individuals should have greater control over the use of data about them.[5]

27. The DFF principles apply to the regulation of all data, including personal information, and align with Cabinet's objectives. They provide, therefore, a further helpful lens when assessing options. The principles of trust and control, in particular, contribute to Cabinet's objective (a), while the principle of value reflects Cabinet objective (b). The principle of inclusion, meanwhile, is a likely result of Cabinet's objectives being achieved.

28. We have used the following criteria to evaluate the options and assess to what extent they contribute to the objectives. Additional criteria assess the impact of other relevant considerations, such as financial implications.

Criteria	Link to objectives, or reason for inclusion otherwise
Ease of understanding and implementation by agencies	The easier agencies find options to understand and implement, the more effective they will be. This will contribute to public trust that information shared with private public sector agencies will be adequately protected.
Impact on agencies (e.g.. improved	The regulation of personal information is likely to impact upon agencies who wish to use personal

[5] Cabinet has agreed that these principles provide a strong framework for a trusted data-use environment that delivers value to all New Zealanders and should underpin approaches to data use in New Zealand"

outcomes, compliance and opportunity costs	information to provide goods and services. Costs need to be demonstrated as being reasonable relative to their impact, such as the likelihood of improved outcomes for agencies.
Impact on individuals (e.g. improved outcomes, decreased likelihood of harm occurring)	The reduction of privacy harms is necessary for individuals to have confidence that information shared with private and public sector agencies will be adequately protected. Furthermore, the easier it is for individuals to understand regulations, the more likely they will be able to exercise their rights. Being able to exercise their rights will increase public trust in innovative uses of data for public good purposes and contribute to public inclusion in the regime. It will also contribute to the identification of problems, which can then be addressed.
Impact on OPC (e.g. resource implications, connections to existing functions)	As the industry regulator with finite resources, capacity, costs accruing to OPC from new regulations need to be considered, though these costs are likely to be operational in nature rather than 'compliance'.
Financial implications for the Crown	
Consistency with existing legislative framework and/or Cabinet decisions	The policy direction of current privacy reforms have already been set by Cabinet, moving away from this direction is likely to create confusion and undermine the consistency of the regime.

PART I: Regulating de-identified information

Problem definition

29. De-identified information is not only valuable from a commercial perspective, but also from a social (e.g. protecting personal information), economic (e.g. protecting risks around identity theft and crime), and policy (e.g. increasing use/re-use of data in evidence-based policy-making) perspective.

30. The ever-increasing sophistication of data technology, however, means that despite best efforts to de-identify information before releasing it, there is always

a risk that downstream third parties may (inadvertently or deliberately) re-identify individuals in a dataset. Re-identification can occur when a second database is combined with de-identified data to reveal personal information. Furthermore, the second database may be of purely non-personal information.

31. De-identified information that has been re-identified by downstream third parties is becoming a major source of privacy harm in other jurisdictions. Appendix 1 summarises prominent examples.

32. A 2015 UK Report of the Independent Surveillance Review noted high levels of public concern about this matter, with 2014 research by the Information Commissioner's Office indicating that 85% of surveyed consumers felt concerned about the manner in which their personal information is passed or sold to other organisations and 77% were concerned about inadequate protection of that information.

33. As the Act was introduced before issues relating to de-identified information were apparent, existing provisions in the Act do not effectively or comprehensively address them.

34. The EU relies on legislative restraints on the de-identification side of the issue for privacy protection. It is unclear how effective this approach is. The US Federal Trade Commission(FTC), on the other hand, has published a privacy framework that:

    34.1. expects agencies should publicly commit to maintain and use data in a de-identified fashion and not attempt to re-identify the data

    34.2. if the company makes de-identified data available to other companies (service providers or third parties) it should contractually prohibit such entities from attempting to re-identify the data.

35. This extent of the problem in New Zealand is not yet known but it is reasonable to assume that it may eventually become significant. This is because of the increasing value of personal information which can sometimes only be obtained by re-identification means. The FTC notes that the commercially valuable nature of re-identified information is one of the reasons it published its framework. Moreover, due to New Zealand's small population (which makes re-identification easier/more likely), it could possibly become a more significant problem than it is overseas.

36. A 2015 resolution by the UN General Assembly on the right to privacy in the digital age noted the rapid pace of technological development and the potential for the aggregation of certain types of metadata to reveal personal information (resolution A/HRC/28/L.27, 24 March 2015). Arising from this resolution, the UN General Assembly has appointed the first Special Rapporteur on the Right to Privacy whose mandate includes making recommendations that respond to the challenges to the right to privacy brought about by evolving technologies.

37. Re-identification has the potential to cause harm and damage public trust in how government and business handles the data of individuals. These are the sorts of outcomes that potentially undermine public service delivery and disrupt a workable framework for the protection of personal information.

38. This paper assesses options that regulate both agencies that de-identify information, and agencies that attempt to re-identify information. As the recommendation made in relation to agencies that de-identify data can be carried out without a Cabinet mandate, it is not included in the Cabinet paper associated with this RIS.

Options for regulating agencies that de-identify information, so that it will be harder for agencies to re-identify that information

39. We have identified three options for regulating agencies that disclose de-identified information:

- *Option 1 - Status quo*: Relying on existing IPPs, such as:
    - IPP 5; which requires agencies that hold personal information to ensure the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against (in particular) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and other misuse, and
    - IPP 11, which requires agencies to consider "on reasonable grounds" that, before disclosure, the information is to be used in a form in which the individual concerned is not identified; or is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.
- *Option 2 - Enhancing the status quo*: non-regulatory approach including leaving the existing IPPs as they are, clarifying that 'other misuse' of data can include re-identification and relying on guidance and assistance with best practice which can be developed by the Privacy Commissioner, including reference to Statistics NZ '5 safes' approach http://www.stats.govt.nz/about_us/who-we-are/policies-and-protocols/microdata-access-protocols.aspx.
- *Option 3 - Amending existing IPPs (either in the Act or by a Code of Practice)*: to make it explicit that it encompasses the need for agencies to take reasonable steps to ensure that their de-identification of personal information is robust enough to withstand attempts at re-identification
- *Option 4* – requiring a privacy impact assessment (PIA) prior to any disclosure of de-identified information.

40. Assessment of these options against our criteria is tabled below

Criteria	Option 1: status quo (using existing IPPs)	Option 2: non-regulatory enhancement of status quo	Option 3: amend existing IPPs	Option 4: PIA prior to disclosure
Ease of understanding & implementation for agencies	• Relying on existing provisions should be easier for agencies, but requires that they already understand risks associated with publishing de-identified data	• Coupling existing provisions with new guidance would likely contribute most to ease of understanding for agencies • Given the complexity of safely de-identifying data, including technical statistical aspects, new guidance would be the minimum essential to encourage safe practice by agencies	• Clear expectation will make due diligence and compliance more straightforward	• Unclear how it would be mandated to best effect. • Easy to understand: Privacy impact assessment is a straightforward and well-established method of risk assessment.
Impact on agencies	• Without explicit expectations or standards across the sector, greater costs to agencies in determining appropriate steps to mitigate risk • Costs for agencies from inadequate risk assessment i.e. reputational issues from failing to take appropriate precautions in de-identifying personal information.	• Clear guidance will make complying with best practice easier for agencies	• May stifle the releasing of valuable data by engendering conservative practices • Would provide greater clarity for agencies to increase confidence in releasing de-identified information • Agencies will likely need to put in place a policy framework to ensure compliance	• Moderate compliance costs for agencies. PIA is a risk assessment methodology that does not require, but can benefit from, professional assistance which may have cost implications. May be costs associated with an agency's first impact assessment but costs likely to reduce on further use of this methodology as familiarity increases.
Impact on individuals	• Would not contribute to inclusion of individuals by making it clear that de-identification is something that agencies should be concerned about safeguarding • May result in privacy harms	• while individuals will be able to access OPC guidance, expectations will not be as prominent as they would be in legislation, implicating public inclusion	• Would make it clear to individuals what expectations are placed on agencies	• Would contribute to inclusion of individuals due to transparency from PIAs being publicised

	and reputational issues for agencies if they do not put in place proper safeguards			
Impact on OPC	• May make it difficult for OPC to investigate or issue compliance notices for bad practices, as no explicit expectation set • May be increased costs associated with responding to or commenting on de-identification failures	• Issuing guidance would mean costs for OPC, but as such activity is within its existing functions, it shouldn't be significant	• Would provide clarity for OPC around investigations and issuing of compliance notices • Likely to require OPC to consider issuing guidance	• Moderate compliance costs for OPC. OPC typically does not formally approve PIA reports but has a well-established role providing assistance to agencies producing them and reviewing the final report.
Financial implications	• Nil	• Nil – No additional costs for OPC, as funding already held in contingency for OPC guidance to support the Bill	• Nil	• Nil
Consistency with Act & Cabinet decisions	• Not previously considered by CAB, or included in the Act, but is consistent with Government objective of less regulation in statute • Should also be considered in light of Cabinet decisions on open data and DFF	• Not previously considered by CAB, or included in the Act, but is consistent with Government objective of less regulation in statute • Should also be considered in light of Cabinet decisions on open data and DFF	• Not previously considered by CAB, or included in the Act. Is not consistent with Government objective of less regulation in statute, but is consistent with framework of Act, which includes specific examples of issues where agencies should have regard • Should also be considered in light of Cabinet decisions on open data and DFF	
Summary of analysis and recommendation	On balance, we consider existing provisions should remain, but they should be coupled with guidance from the OPC (option 2). Option 2 most effectively balances the objectives of providing confidence to the public – by shoring up trust in the regime – while also not placing an undue chilling effect on agencies who may hold data that would provide public value if released in de-identified form.			

Options for regulating agencies that attempt to re-identify information

41. The following options have been considered to ensure appropriate protection of de-identified information, and are assessed in the table below:

    - *Option 1 Status quo*: no regulation of re-identification practices
    - *Option 2 Code of Practice:* to modify relevant information privacy principles and specify how re-identified information may be used
    - *Option 3 amend IPPs 10 and 11*: to specify how re-identified information may be used and disclosed
    - *Option 4 a new IPP:* to explicitly state that agencies that acquire de-identified information must not take deliberate attempts to re-identify that information and must not act on inadvertently re-identified data. Limited exceptions will apply.

42. Assessment of these options against our criteria are tabled below:

Criteria	Option 1: Status quo	Option 2: Code of practice	Option 3: Amend IPPs 10 & 11	Option 4: a new IPP
Ease of understanding & implementation for agencies	• As an emerging issue, the status quo is likely to mean that the issues surrounding the use of re-identified data are not adequately understood by agencies, which will therefore be unable to manage risks	• A code is developed in consultation with all relevant stakeholders, likely including representatives of the public, which will contribute to an ease of understanding and implementation	• Would be functional and would provide more authority than a Code • Does not fit very well within the existing IPPs, as, re-identification is neither use or disclosure • Could create confusion, as the risk of re-identification involves different agencies at different points in the life-cycle of information	• A new IPP would fit with the "life-cycle of information" approach already taken by the IPPs • Easier to work with and less likely to make existing provisions more difficult to work with • More likely to provide appropriate level of authority • Given the complex nature of the issues (e.g. boundaries between "identified" "de-identified" and "re-identified") a new principle alone may not be sufficient to ensure ease of understanding. A new IPP would benefit from legislative definitions and additional guidance to ensure ease of understanding.

Impact on agencies	• costs will be individualised to each agency depending on risk assessment and awareness of reputational issues	• the loss of commercial benefit that agencies could gain from re-identifying personal information will be offset by alternative commercial benefits that accrue from the appropriate use of larger and better quality data sets that will result from greater public trust in the use of de-identified data • marginal increase for agencies to determine whether actions might inadvertently lead to personal information being re-identified	• the loss of commercial benefit that agencies could gain from re-identifying personal information will be offset by alternative commercial benefits that accrue from the appropriate use of larger and better quality data sets that will result from greater public trust in the use of de-identified data • marginal increase in compliance costs as agencies will need to become familiar with manner in which re-identified information may be used • further marginal increase for agencies to determine whether actions might inadvertently lead to personal information being re-identified outside of what is allowed	• the loss of commercial benefit that agencies could gain from re-identifying personal information will be offset by alternative commercial benefits that accrue from the appropriate use of larger and better quality data sets that will result from greater public trust in the use of de-identified data • marginal increase for agencies to determine whether actions might inadvertently lead to personal information being re-identified
Impact on individuals	• may contribute to privacy harm as it does not incentivise agencies to adopt good privacy practices in a fast- paced information- driven world			

Impact on OPC	• Responding to incidents and failures	• developing a Code is time and resource intensive for OPC • would add to OPC's reporting requirements, as it will be required to report on operation of Code annually	• nil - improper practice relating to re-identified data are already in regulatory ambit of Commissioner's powers	• nil - improper practice relating to re-identified data are already in regulatory ambit of Commissioner's powers
Financial implications	• Nil	• Due to significant cost to develop, OPC may seek additional funding	• Nil	• Nil
Consistency with Act & Cabinet decisions	• would undermine Cabinet's objectives to ensure that individuals have confidence that information shared with private public sector agencies will be adequately protected		• does not fit with the "life-cycle of information" approach already taken by the IPPs, and thus would complicate existing (and already complex) provisions	• good fit with the "life-cycle of information" approach already taken by the IPPs
Summary of analysis and recommendation	On balance, legislative amendment is recommended over either the status quo or a Code of Practice. The status quo is discounted due to the risks it poses. A code is discounted due to the significant costs that would accrue to OPC during its development, without providing any value regulatory value over and above a legislative change. Of the two legislative options, a new IPP (option 4) is recommended. As re-identified information constitutes a distinct stage of the life-cycle of personal information, it is not appropriate for already existing exceptions to be modified. A new IPP is likely to be easier and clearer for agencies to work with, compared to cluttering already complex existing provisions. Given the complex nature of the issues (e.g. boundaries between "identified" "de-identified" and "re-identified"), however, a new IPP alone may not be sufficient to ensure ease of understanding, and would benefit from legislative definitions and additional guidance to ensure ease of understanding.			

PART II: Refining previous decisions about mandatory breach notification

Problem definition

43. During the legislative drafting of decisions relating to mandatory breach notification, the following three problem areas were identified:

    43.1. agreed exceptions to the requirement to notify individuals of serious breaches do not provide agencies with the necessary clarity about when exceptions should apply, and the list of exceptions is not consistent with other provisions

    43.2. the threshold for notifying the Commissioner of a material breach do not provide agencies with the necessary clarity for them to know when to do so

    43.3. affected individuals do not have the right to complain to the Commissioner if an agency fails to notify them of a serious breach.

44. The first two of these problems, if not resolved, have the potential to affect every agency that holds personal information. They will make complying with mandatory breach notification requirements more difficult for agencies and add transaction costs.

45. The last problem, if not resolved, will impact upon the proper functioning of the new regime – that is, protecting individuals from privacy harm. In particular, a penalty for failing to notify an individual of a serious breach is necessary to ensure agencies are properly incentivised to inform individuals of a serious breach. Agencies need to be incentivised to notify individuals to subsequently encourage them to then take any necessary actions, and also allow individuals the opportunity, to minimise the harm.

Clarifying and extending exceptions to the requirement to notify affected individuals

The issue

46. While the Bill introduces an obligation on agencies to notify individuals of serious breaches, there will be some exceptions. Cabinet agreed that agencies will not have to notify individuals to "*protect trade secrets, security, and/or vulnerable individuals*."

47. As they are currently written, these exceptions are not consistent with the existing legislative framework. In particular, they are worded differently and, in comparison with the other exceptions, do not provide adequate clarity about when they apply. Comparison with already existing exceptions has also indicated that the exceptions to notifying individuals of serious breaches are not comprehensive.

48. After assessing exceptions included in other provisions, we consider an additional exception should be included, to avoid prejudicing the maintenance of the law by a public sector agency, including the prevention, detection, investigation or prosecution of offences and the right to a fair trial.

49. Considering the content and intent of previous Cabinet decisions, only two options are presented here.

The options

50. The options are to either:

    50.1. Option 1: Leave the exceptions as agreed by Cabinet

    50.2. Option 2: the exceptions should be expanded to align with other provisions in the Act, or to clarify Cabinet's intent, as below:

- notification might:

    a. [*agreed by Cabinet in 2014 and improved for clarity*] prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand

    b. [*new*] prejudice the maintenance of the law by a public sector agency, including the prevention, detection, investigation or prosecution of offences and the right to a fair trial

    c. [*agreed by Cabinet in 2014 and improved for clarity*] endanger the life or health of the individual concerned

    d. [*agreed by Cabinet in 2014*] reveal a trade secret[6]

- [*agreed by Cabinet in 2014 and improved for clarity*] the agency considers on reasonable grounds that notification:

    e. would be likely to prejudice the physical or mental health of an individual; OR

    f. in the case of an individual under 16, would be contrary to that individual's interests.7

51. Assessment of these options against the criteria is tabled below:

	Option 1: Status quo (as agreed by Cabinet)	Option 2: expanded and comprehensive consistent with Act
Ease of understanding & implementation for agencies	• Insufficient flexibility provided by current list of exceptions to notification	• adds appropriate flexibility by way of additional exceptions
Impact on agencies	• Diverging from established wording could create confusion for agencies	• less ambiguity for agencies

[6] b. and d. are based on exceptions contained in IPPs 2, 3, 10, 11. c. is based on exceptions contained in IPPs 10, 11. a. is based on Part 4, section 27 of the Privacy Act.

[7] e. and f. are based on Part 4, section 29 of the Privacy Act.

Impact on individuals	• The situations where agencies could rely on the exceptions would be less clear, potentially leading to inappropriate applications that impact on individuals	• individuals would have a clearer understanding of when exceptions may apply to them
Impact on OPC	• Nil	• Nil
Financial implications	• Nil	• Nil
Consistency with Act & Cabinet decisions	• Consistent with previous Cabinet decisions, but not with existing legislative framework	• Consistent with intent of previous Cabinet decisions, and with existing legislative framework
Summary and recommendation	On balance, it makes sense to clarify and expand what was previously agreed by Cabinet. Expanding the list of exceptions to notification provides the necessary flexibility for the breach notification framework and reduces risk of notification being made in situations where notification may exacerbate harm or prejudice other important public or personal interests.	

Clarifying the numeric threshold for notifying the Commissioner of a material breach to provide agencies with the necessary clarity for them to know when to do so

The issue

52. Cabinet has agreed that agencies, when determining whether a material breach has occurred, will have regard to certain trigger factors such as (i) "the number of people" involved in the incident (ii) the sensitivity of the information and (iii) indications that the breach was caused by a systemic problem). If a material breach has occurred, an agency must notify the Commissioner.[8]

53. The first trigger factor (the "number of people"), however, does not provide agencies with as much clarity as it would if a specific number was prescribed. The following analysis, therefore, assess whether to set a specific number.

54. The analysis concludes that a specific number should be set. The issue of what that number should be is discussed following the analysis.

Options analysis: whether or not to set a specific number?

55. The options are:

    55.1. Option 1: Status quo – unspecified numeric trigger "number of people"

    55.2. Option 2: Setting a specific numeric trigger by legislative instrument.

56. Assessment of these options against the criteria is tabled below:

[8] The number only applies to a material breach, where no harm has been caused. Where harm is caused the breach is considered serious agencies are required to take reasonable steps to notify the Commissioner and affected individuals (without regard for number of affected), unless an exception applies.

	Option 1: Status quo: unspecified numeric trigger: "number of people"	Option 2: Setting a specific numeric trigger by legislative instrument.
Ease of understanding & implementation for agencies	• Requires more judgement by agencies • May contribute to situations where agencies do not notify the Commissioner when they should (because there is a risk that agencies will over-estimate the number of people relevant to a material breach) • Will make it easier for OPC, during investigations, to determine whether agencies acted reasonable in deciding not to notify the Commissioner of a material breach	• Will provide agencies with a better understanding of when to notify the Commissioner of a material breach • In theory, having a specific threshold may undermine the other factors agencies must also have regard for. i.e. if the number of affected people falls below the threshold, agencies might not consider the other factors. In practice, however, agencies will be required to consider all factors. The Bill will be drafted to make this clear.
Impact on agencies	• No new compliance costs - agencies will already need to comply with new mandatory breach notification provisions	• No new compliance costs - agencies will already need to comply with new mandatory breach notification provisions
Impact on individuals	• N/A	• N/A
Impact on OPC	• Nil	• Nil
Financial implications	• Nil	• Nil
Consistency with Act &/or Cabinet decisions	• Consistent with Cabinet intent	• Consistent with Cabinet intent
Summary and recommendation	On balance, we consider setting a specific number of people relevant to a material breach is the best option. In particular, we consider that without a specific number that can be easily referenced, agencies are unlikely to have a good idea what constitutes a material breach, which opens them up to an unnecessary risk of receiving a substantial fine ($10,000).	

Determining the specific number that agencies should have regard for

57. There is limited evidence for determining how many people are relevant to a material breach. Due to the voluntary nature of the existing notification regime, there is not a consistent body of knowledge about the number of breaches that currently occur, or the number of individuals implicated in each breach. Nor are there any precedents or similar provisions that can inform the number.

58. The lack of evidence makes it difficult to set the specific number before the new regime of mandatory breach notification is established. Once the mandatory regime is in place, however, with a specific number that agencies should have regard for, OPC will be able to measure the appropriateness of that number with regard for the appropriate level of protections afforded the public and the resource implications for OPC.

59. For this to take place, an initial number needs to be set, which can be reviewed once the necessary level of evidence has been gathered through the normal operation of the mandatory breach regime. This number will be set in close consultation with OPC, based on assessments of the resource implications for OPC, the compliance burden for agencies, and appropriate protections afforded to the public.

60. This approach presumes that the number will be able to be changed at a later date, if necessary. This means that the manner in which this number is set in regulation needs to be considered. In particular, should the number be set in primary legislation, or is it more appropriate for it to be set in regulation with an accompanying regulation making power?

61. The flexibility of a regulation-making power is considered to be appropriate, as the decision about what the number should be is mostly an administrative decision that does not require Parliament's oversight. This is especially so considering the number will be set based on the advice of OPC following its assessment of the regime.

Determining if affected individuals should have the right to complain to the Commissioner if an agency fails to notify them of a serious breach

The issue

62. In 2014 Cabinet agreed to a financial penalty for failing to notify the Commissioner of either a material or serious breach. It was anticipated that the Commissioner would issue a compliance notice if agencies failed to notify affected individuals of a serious breach. Cabinet therefore discounted including a financial penalty for failing to notify an individual of a serious breach.

63. Upon drafting, however, it was noted that while the Commissioner can issue a compliance notice to an agency for failing to notify an individual of a serious breach, this will not provide a remedy to an affected individual. As failing to notify an individual of a serious breach directly impacts upon the affected individual, we now consider that the individual should have recourse to complain to the Commissioner and seek a remedy from the agency concerned or via the Human Rights Review Tribunal.

64. A mechanism for individuals to complain to the Commissioner in certain situations already exists in the Act. These situations are considered "interferences with privacy". If it is considered appropriate that individuals should have the right to complain to the Commissioner for failing to be notified of a serious breach where this has adverse consequences for the individual concerned, this situation would be added to the Privacy Act's definition of "interference with privacy"..

65. While an individual can already complain about a data breach (that causes harm), under this proposal the individual could bring an *additional* complaint that the failure to notify had caused further harm (i.e. made the harm from the breach worse – for example, if the person had known earlier they could have changed their password).

The options

66. The following options are therefore considered:

    66.1. *Option 1 - status quo*: no complaint ground for individuals where failure to notify a serious breach

66.2. *Option 2* - provide a complaint ground for individuals where failure to notify a serious breach

Assessment of these options against the criteria is tabled below:

	Option 1: Status quo	Option 2: provide ground of complaint
Ease of understanding & implementation for agencies	• Individuals may assume a right of complaint when there is not one	• Consistent with how individuals can complain and seek remedies for other breaches of the Act that have adverse consequences for individuals
Impact on agencies	• No compliance costs for agencies • Less incentive for agencies to notify individuals affected by a serious breach (subject to the use of other regulatory tools such as compliance notices)	• Upfront, there will be no new compliance costs, as agencies are already required to notify individuals of a serious breach. Downstream, however, agencies may need to be involved with Commissioner investigations, as individuals will have recourse to make a complaint
Impact on individuals	• Individuals will not be able to complain about, and seek remedy for, an agency breach that has had adverse consequences • Not including this right to complain will lead to less inclusion of individuals in regime, and likely lead to more privacy harms	• Individuals can complain to the Commissioner and seek a remedy from the agency concerned or via the Human Rights Review Tribunal
Impact on OPC	• Nil	• Impact on OPC not clear but may not be large as OPC already aware of issue through notification and potential to utilise compliance notice power
Financial implications	• Nil	• Unknown, will depend on how many complaints made to Commissioner – as yet no evidence on which to base this
Consistency with Act &/or Cabinet decisions	• Is not consistent with Cabinet objective that individuals have confidence that information shared with private public sector agencies will be adequately protected	• In line with purpose of the Act and previous Cabinet intent, agencies will be incentivised to notify so that harm can be mitigated
Summary and	On balance, providing complaint rights for failure to notify an individual	

recommendation	of a serious breach is appropriate. The status quo is discounted due to the lack of inclusion of individuals in the regime it represents, and subsequent increased likelihood of privacy harm, which will undermine the purpose of the Privacy Act and Cabinet objectives. The ability for individuals to make a complaint to the Commissioner is necessary to ensure that they can be properly involved at appropriate points in the regime.

Consultation

67. The Law Commission consulted extensively during the development of its 2012 report with both public and private agencies. This included consultation with individuals, private sector businesses, non-government organisations, and public sector agencies (including the Office of the Privacy Commissioner).

68. 2014 Cabinet decisions were broadly consistent with the Law Commission recommendations. and incorporated further extensive consultation with the private and public sector, carried out by the Ministry of Justice.

69. As proposals contained in this paper remain in line with the intent of Cabinet's 2014 decisions, consultation on this paper has been more focused. We have, however, remained in close consultation with the Office of the Privacy Commissioner and the Data Futures Partnership.

70. The following agencies have been consulted on this RIS: Accident Compensation Corporation, Crown Law, Ministry for Culture and Heritage, Customs, Civil Aviation Authority, Ministry of Defence, Department of Conservation, Housing New Zealand, Human Rights Commission, Department of Prime Minister and Cabinet, Department of Internal Affairs, Ministry of Education, Department of Corrections, Office of Human Rights Proceedings, Ministry of Health, New Zealand Security Intelligence Service, Government Communications Security Bureau, Land Information New Zealand, Inland Revenue Department, Maritime New Zealand, Ministry for Pacific Peoples, Ministry for Primary Industries, Ministry of Foreign Affairs and Trade, Ministry of Business, Innovation and Employment, Ministry of Social Development, Ministry for the Environment, Office of the Ombudsman, Office of the Clerk of the House of Representatives, Office of the Privacy Commissioner, Office of the Attorney-General, Parliamentary Service, Parliamentary Counsel Office, New Zealand Police, Reserve Bank of New Zealand, State Services Commission, Serious Fraud Office, Statistics New Zealand, Data Futures Partnership, Treasury, Ministry of Transport, New Zealand Transport Authority, and Te Puni Kōkiri.

71. A wider range of actors will be given the opportunity to comment on these amendments during Select Committee.

72. The original Data Futures Forum proposal to regulate against re-identification was based on targeted engagement across sectors. However the Forum did not consult on the specific proposal. No further public consultation has been undertaken on the proposals relating to de-identified and re-identified data.

Conclusions and recommendations

Regulating de-identified information

73. The Ministry considers that existing legislative provisions are adequate for regulating agencies that de-identify personal information, but should be coupled with new guidance from the OPC. We consider this adequately balances compliance costs for agencies against the desire for agencies to make available information that has public value.

74. The Ministry also considers a new IPP should be introduced regulating agencies to explicitly state that agencies that acquire de-identified information must not take deliberate attempts to re-identify that information, and must not act on inadvertently re-identified data (with limited exceptions). Given the extent of potential privacy harms that may occur if agencies are not prohibited from these activities, it is appropriate for such a prohibition to be included in legislation. Furthermore, given the existing IPP framework, it is best that this is included as a new IPP. We also consider guidance from OPC would ensure proper understanding of the new provisions.

Refining previous decisions about mandatory breach notification

75. The Ministry recommends that the following changes should be made to mandatory breach notification provisions. These options are considered to best meet the objective of ensuring public confidence in how agencies handle their personal information, thus contributing to the objective of agencies being able to access the information they need to provide goods and services as effectively as possible:

    75.1. exceptions to the requirement to notify individuals of serious breaches should be clarified and expanded in line with other exceptions contained in the Privacy Act;

    75.2. a numerical threshold for notifying the Commissioner of a material breach should be introduced to provide agencies with the necessary clarity for them to know when to do so; and

    75.3. affected individuals should have the right to complain to the Commissioner if an agency fails to notify them of a serious breach.

Implementation

76. OPC will lead the implementation of the operational proposals contained in the package of privacy reforms; working closely with the Ministry of Justice and other relevant parties to ensure that the policy intent is appropriately implemented.

77. The Ministry of Justice, in conjunction with OPC, will consult with relevant agencies to determine what number should be set helping to determine whether a material breach has occurred. See paragraphs 51 – 60 above.

78. OPC will enforce the new laws from the date they come into force. We are proposing the Act will come into force 6 months after assent. This will provide agencies with the time needed to prepare for new procedures.

Monitoring, evaluation and review

79. Government has introduced a regulatory scanning programme, overseen by Treasury. This involves the systematic evaluation of an agency's legislation and regulations. There is an annual reporting cycle for regulatory scanning.

80. The Ministry of Justice scans groups of legislation for which it is responsible as part of a "rolling programme", with the aim that all regulation is scanned at regular intervals. The Act will be part of this programme. The Ministry will consult relevant stakeholders including the Commissioner.

81. The Act operates in a highly changeable environment with technology and international developments suggesting that the Act may need to be reviewed more frequently than every five years.

82. Section 24 of the Act requires the Commissioner to report on the operation of the Act. Once the proposed initiatives are in force, OPC will be able to gather and report on data with respect to:

    82.1. the number and size of breaches, by type of breach (serious, material)

    82.2. the number of compliance notices, by type of notice, and outcomes

    82.3. the number of own motion investigations, by type of issue detected, and outcomes.

83. This data will be able to be used, in particular, to assess whether the number set to help determine whether a material breach has occurred is set at the right level. See paragraphs 51 – 60 above.

84. The Privacy Commissioner will record and publish statistical information on material data breaches received in his or her annual report. After 24 months or at any time before the Commissioner may make a recommendation to the Minister about whether the process is working satisfactorily and whether any changes are necessary and desirable, which would include a recommendation as to whether the threshold number should be raised, or lowered. At any stage he may recommend to the Minister that the Ministry should conduct additional research or should commission an external review.

Appendix 1

1. **GIC -** In 2009 the Group Insurance Commission (GIC) released anonymised data on state employees that showed every hospital visit. William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers.

   In response, then-graduate student Latanya Sweeney started hunting for the Governor's hospital records in the GIC data. She knew that Governor Weld resided in Cambridge, Massachusetts, a city of 54,000 residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge, a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor Weld with ease. Only six people in Cambridge shared his birth date, only three of them men, and of them, only he lived in his ZIP code.

   Dr. Sweeney sent the Governor's health records (which included diagnoses and prescriptions) to his office. http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin

2. **AOL** - (an ISP provider) released thirty-six million search queries made over the course of three months by five hundred thousand of their users. They replaced the usernames with ID numbers. That was not enough to shield the identities of the users. Journalists quickly found out that the data itself might well be de-identified, but individual users could still be tracked down after looking through their set of search terms (http://www.pentadact.com/2006-08-09-aolol/ and http://arstechnica.com/business/2006/09/7835/ refer).

   AOL is now required to pay for a year of credit monitoring for all users whose data was posted and send such users a certified letter notifying them that their data was made public.

3. **Netflix** - Narayanan. A. and Shmatikov. V. *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*. 5 February 2008. University of Texas at Austin – (http://arxiv.org/pdf/cs/0610105.pdf and http://arstechnica.com/tech-policy/2009/03/pulling-back-the-curtain-on-anonymous-twitterers/ refer).

   The authors cross-correlated non-anonymous records from the Internet Movie Database with anonymized Netflix records and discovered that it was possible to learn sensitive non-public information about a person's political or even sexual preferences.

4. **Twitter** - Narayanan and Shmatikov's subsequent paper, *De-anonymizing social networks*, is another attack on the idea that data can be easily anonymized by stripping out a few bits of personally identifiable information (PII). Much of their work over the last few years is built on the premise that PII extends far beyond names and addresses; in many datasets, the very structure of the data provides all sorts of clues that can be deciphered with only a few bits of information.

   The authors took an anonymous graph of the social relationships established through Twitter and find that they can actually identify many Twitter accounts based on an entirely different data source—in this case, Flickr.

One-third of users with accounts on both services could be identified on Twitter based on their Flickr connections, even when the Twitter social graph being used was completely anonymous. The point, say the authors, is that "anonymity is not sufficient for privacy when dealing with social networks," since their scheme relies only on a social network's topology to make the identification.

The issue is of more than academic interest, as social networks now routinely release such anonymous social graphs to advertisers and third-party apps, and government and academic researchers ask for such data to conduct research. But the data isn't nearly as "anonymous" as those releasing it appear to think it is, and it can easily be cross-referenced to other data sets to expose user identities.

It's not just about Twitter, either. Twitter was a proof of concept, but the idea extends to any sort of social network: phone call records, healthcare records, academic sociological datasets, etc.