LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

MINISTERIAL BRIEFING

INFORMATION SHARING

29 MARCH 2011

Information Sharing

INTRODUCTION

1. The Law Commission is currently engaged in a review of the Law of Privacy. The work is proceeding in four stages. The first three stages are complete,[1] and the Commission will soon complete the fourth and final stage, a review of the Privacy Act 1993. It published an Issues Paper on the subject in 2010,[2] and is presently writing its final report. That report is due for publication by mid-year 2011.

2. In the course of the review of the Privacy Act we were asked to study the sharing of personal information between government agencies. The question is the extent to which a government agency that holds personal information about an individual is justified in disclosing that information to another agency. There has been uncertainty and debate about this subject for a number of years. Sharing is lawful now if it comes within one of the exceptions to the Privacy Act principles. Unfortunately, however, it is not always easy to get agreement between agencies on what is permissible and what is not. The whole-of-government solutions which can be facilitated by information sharing have attractions in many contexts, but they do have implications for the privacy of the individual, and it is no easy task to get the balance right.

3. In its Issues Paper on the review of the Privacy Act the Commission reviewed the literature and overseas developments, and put forward a number of options for taking the matter forward in this country. That work is contained in Chapter 10 of the Issues Paper. We received some helpful submissions on the options presented there. We have also consulted government agencies and others, and organised and participated in a number of forums where we put forward for comment the conclusions we have arrived at. We have also met, and exchanged ideas, with a group convened by the State Services Commission which has been working on the same topic.

4. Our conclusions and recommendations will be contained in a chapter of our final

---

[1] Stage one of the review of the Law of Privacy was a high-level analysis to assess privacy values, changes in technology, international trends, and their implications for New Zealand law. Stage two was a consideration of the law relating to Public Registers and whether it requires systematic alteration as a result of privacy considerations and emerging technology. Stage three considered the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy.

[2] Law Commission *Review of the Privacy Act 1993* (NZLC IP 17, 2010).

report on the review of the Privacy Act. However there is some urgency in the matter of information sharing, and we have been requested by the Minister Responsible for the Law Commission to present our conclusions, and eventual recommendations, in advance of that final report. This paper, which takes the form of policy advice to the Minister, fulfils that purpose.

5. In this paper we set out the reasons we believe reform of the law is required, and the principles on which that reform should be based. After discussing other options, we introduce our preferred option and discuss it in some detail. This is the "approved sharing programme". Sharing arrangements between agencies would go through an approval process culminating in approval by Order in Council, and would be listed in a schedule to the Privacy Act. The approval process would ensure that there was clarity as to what information could be disclosed, and that proper safeguards were in place to protect the privacy of the individual.

DEFINITION

6. We define the term "sharing" broadly as the disclosure of personal information about an individual by one agency to another. It can take many forms, including:
   - A reciprocal exchange of information between agencies.
   - One or more agencies providing information to another agency.
   - Several agencies pooling information (as in a common database) and making it available to each other.
7. The physical ability of agencies to share information about citizens has been greatly enhanced in recent times. This is an area where technological advances are hugely significant. The difficulties of locating and sharing personal information between public sector agencies that exist when the information is stored in individual paper files held in each agency are swept away when the information is held in digital form and is accessible remotely from anywhere, without the need to physically transfer the information from agency to agency. Government agencies want to use this technology to deliver better services more efficiently. Collaboration between agencies using shared information can often provide such better, "smarter" services.
8. A number of sharing programmes operate now. An example is the Linwood Service Centre in Christchurch where a number of agencies, including Work and Income, Career Services, Housing New Zealand, the Ministry of Health and the Ministry of

Education work together to provide services for individuals and/or families with multiple service needs. Another is the Priority Offenders Initiative where Police, Probation and Prison Re-integration Officers, Housing New Zealand, Ministry of Education, Child, Youth and Family, Ministry of Health and Work and Income provide services in relation to frequent offenders who commit a disproportionate amount of crime in their local area. Another example, different again, is the projected Joint Border Management System (JBMS) which is designed for the collection, storage and use of border information by the New Zealand Customs Service and the Ministry of Agriculture and Forestry.[3]

9. It will be immediately clear that the purposes of such arrangements, and the risks involved in them, differ considerably from one to another. Some focus exclusively on benefit to individuals and families; others are designed to benefit the community as a whole by preventing or detecting wrongdoing; others involve a mixture of both. Even in programmes that are ostensibly for the benefit of individuals things adverse to an individual may come to light to which the authorities cannot realistically be expected to turn a blind eye. There are difficulties, even dangers, in trying to classify sharing arrangements into pre-ordained categories.

10. As we shall explain in more detail later,[4] we think information matching, long regarded as a special type of activity subject to its own closely regulated regime, is really a form of sharing. We regard information sharing as a spectrum of different types of activity of which matching is one.

11. We note also that in this paper we are concerned only with sharing of information between *agencies*, and not with sharing between individuals in the *same* agency. That is a different question, albeit one which can raise its own issues, particularly where one agency has merged with another. We regard Privacy Act principles 5 and 10 as providing appropriate protection in that situation, but it may be that the transparency requirements that we propose later in this paper could have useful analogical application there too. We shall discuss intra-agency disclosures further in our report on the Review of the Privacy Act. Nor does our brief extend to sharing between New Zealand government agencies and overseas government agencies. We are concerned

---

[3] As provided for in the Customs and Excise (Joint Border Management Information Sharing and Other Matters) Amendment Bill 2010 which is awaiting its final stages in the House. Other examples of sharing initiatives are given in the Law Commission *Review of the Privacy Act 1993* (LC IP 17, 2010) at [10.18]–[10.32], and in AMB Lips, RR O'Neill and EA Eppel *Improving Information Sharing for Effective Social Outcomes* (VUW, December 2009) at 18−57.

[4] See paragraphs [57]–[61].

solely with sharing within New Zealand.

BENEFITS AND RISKS

12. Information sharing has obvious benefits. For individuals and families some types of sharing can, as in the case of the Linwood Centre, enable integrated assistance. Individuals are relieved of the need to supply the same information to several agencies. The agencies can work together to see and understand the individual's problems in their whole context, instead of each agency seeing only through its own narrowly focused lens. The Government, and therefore society, also benefit from the improved effectiveness of outcomes and from the efficiencies gained. Such activities should be facilitated. Other beneficial outcomes might include the more effective discovery and resolution of debts, and greater speed and certainty in ascertaining benefit entitlements. Sometimes the benefit of a co-ordinated response is so obvious that it goes without saying: the prevention of child abuse is a clear example; dealing with the aftermath of the devastating Christchurch earthquake is another.[5]

13. However the risks of sharing can be considerable and need to be carefully managed. There are significant implications for individual privacy. Sharing, in fact, runs counter to two fundamental principles of the Privacy Act: that personal information should only be collected from the individual concerned, and that information collected for one purpose should not be used for another. Moreover, if information is inaccurate the error will appear in multiple databases, making it more difficult to correct. It may be difficult for individuals to find out exactly where their information is held so that they can take steps to ensure that it is corrected. Moreover some of the information shared can be particularly sensitive, information about finance and personal relationships for instance, and the more hands it passes through the greater the risk of its loss or misuse. Failures of security, the use of inaccurate information, and the use of information in ways which are not anticipated by the individual, can lead to loss of trust in government. The human psyche is instinctively fearful of the "big brother" state. No government can afford to lose the trust of its citizens: it will lead to reluctance to co-operate in providing information in the future.[6]

---

[5] The Privacy Commissioner has issued a temporary code of practice to facilitate sharing in that context: the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary).

[6] In AMB Lips, EA Eppel, A Cunningham and V Hopkins-Burns *Public Attitudes to the Sharing of Personal Information in the Course of Online Public Service Provisions* (VUW, August 2010), the authors report on the results of research into

14. Privacy protection also has international significance. Government practices can have implications for cross-border dealings. As the UK Information Commissioner's Office has recently said: "Not only is personal information shared more often and in greater volume than ever before, but the potential for inadequate information handling systems and practices to have far reaching consequences has also increased dramatically."[7]

15. The authors of the Data Sharing Review Report in the UK sum it up this way:[8]

> Technological advances have had a dramatic impact on data collection and management. Ever larger databases, powerful search and analysis facilities, and the increased (and almost infinite) storage capacity of modern IT systems belong to a very different world from filing cabinets stuffed with paper. It is simple to share, search and interrogate huge datasets electronically, although not so simple to do this safely and securely.

THE NEED FOR REFORM

16. The question, therefore, is how to facilitate information sharing but also to ensure that proper protections and safeguards are in place. Much sharing is possible under the Privacy Act's information privacy principles (IPPs) now. Disclosure of information is often able to be justified as being within one of the exceptions to principle 11 (the non-disclosure principle), examples being the health and safety exception, and the maintenance of law exception.[9] Sharing is also justified if it is within the purpose for which the information was collected, or if the individual concerned has consented. We have heard a view that the Act is adequate as it stands and that with proper guidance the current IPPs are all that is required. We do not agree. It is quite difficult to fit some of the current sharing arrangements into the IPPs; the agencies involved often feel it necessary to get the consent of the individuals concerned rather than rely on the other exceptions. Moreover, the IPPs, and the exceptions to them, are expressed in broad and open-ended terms, as they must be. But this means that they are open to differing interpretations. That is, perhaps, particularly so in the case of the purpose exception,[10] but all of them can from time to time give rise to uncertainty in their

---

public attitudes. They show that reaction depends on context, the extent of the sharing, and the population group in question.

7 Information Commissioner's Office *Response to the Ministry of Justice's call for evidence on the current data protection legislative framework* (6 October 2010) <www.ico.gov.uk/~/media/documents/library> at 2.

8 R Thomas & M Walport *Data Sharing Review Report* (London, 2008) at 44.

9 Privacy Act 1993, s 6, Information Privacy Principle 11.

10 Privacy Act 1993, s 6, Information Privacy Principle 11, and the first exception to it, read:

> An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes,

application.

17. Two things have resulted from this. First, agencies participating in sharing arrangements sometimes disagree on what is permissible and what is not. In our Issues Paper we summarised some of the conclusions reached by researchers from the Victoria University of Wellington:[11]

- Where agencies had a public safety mandate the Privacy Act was not seen as such an obstacle, with Principle 11 seen as providing adequate authority to share information. But in the case of agencies with a public service mandate, there were greater uncertainties as to the application of the Privacy Act. It was not seen as helpful in some cases.
- Overall, there was an awareness among agency staff of the Act's general requirements, but sometimes that awareness was not backed up with detailed knowledge.
- Legal interpretations of the Act differ, and there was sometimes uncertainty about whether the Privacy Commissioner would uphold an agency's decision.

We have heard in the strongest terms from agencies that things are unlikely to improve until there are clear detailed provisions to which agencies can point as justifying their actions.[12] Then there can be no argument as to what can and cannot be accessed. In this regard, Schedule 5 of the Privacy Act is seen as a useful precedent: it lists various types of information relating to law enforcement, and specifies the agencies which may access each type.

18. Secondly, rather than relying on the Privacy Act's existing provisions, some agencies are seeking specific amendments to their own Acts to validate particular sharing programmes. In our Issues Paper, we gave the examples of sections 181A and 182A of the Corrections Act 2004, which provide for information sharing about high-risk offenders and child sex offenders, and section 283 of the Accident Compensation Act 2001, which provides that the Accident Compensation Corporation may provide information about claimants and other persons to the Department of Child, Youth and

---

on reasonable grounds,

(a)that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained;

The concept of the purpose of obtaining (as opposed to collecting) information may not always be crystal clear; 'direct relation' to such a purpose can be a matter on which judgments may differ.

11 See the Law Commission, above n 2, at [10.58]. The Research Report is that referred to in n 3 above.

12 From personal interviews, forums and seminar discussion.

Family Services where that is necessary to protect children and young persons. In 2010 there have been two further examples: a Bill to enable Inland Revenue to share taxation information with other departments,[13] and a Bill to amend the Customs and Excise Act to enable the Customs Service and the Ministry of Agriculture and Forestry to share border information.[14] This process of specific statutory amendment is resource-intensive and time-consuming. In addition, there is currently no authoritative framework for assessing such proposals. The more this happens the more there is a risk of inconsistency and a loss of clear principle.

19. As we indicated above, some of the current sharing programmes operate with the consent of the individual. While this is certainly in accordance with the IPPs, it is not always satisfactory. It is one thing for a person to sign a detailed consent form, but another for that person to fully understand what it is that he or she is supposedly consenting to. We have also had it put to us that imbalance of power can be a significant problem in such cases. Moreover, a programme cannot operate with optimal effect if some individuals refuse their consent.

20. So we are of the view that reform is required to attain greater certainty in this area, and to ensure that proper safeguards are in place. Our aim is to identify a way to facilitate appropriate public sector information sharing within a framework of openness, transparency and accountability, which accords appropriate weight to privacy values.

OVERSEAS DEVELOPMENTS

21. In the Law Commission's Issues Paper[15] we describe developments in information sharing in other jurisdictions similar to our own, with a warning that it can be dangerous to rely too heavily on overseas experience. Laws, and the culture surrounding them, can differ from place to place.

22. We now briefly summarise those developments. A fuller account can be found in the Issues Paper.[16]

23. All jurisdictions allow a disclosure of information which is within the purpose for which it was collected, or which has the consent of the individual. Beyond that, there

---

13 Taxation (Tax Administration and Remedial Matters) Bill 2010 (257-1).

14 Customs and Excise (Joint Border Management Information Sharing and Other Matters) Amendment Bill 2010 (200-2).

15 Law Commission, above n 2.

16 Ibid, at [10.68]–[10.115].

is a great variety of provisions. In the **United Kingdom**, the lack of clarity in the relevant legislation has been a constant theme. A report published in 2008 recommended a statutory duty in the Information Commissioner to publish and update a code of practice relating to information sharing.[17] It also recommended a fast-track legislative procedure which would enable the Secretary of State, in precisely defined circumstances, to make orders removing or modifying barriers to information sharing. Such an order could amend primary legislation where necessary. Both Houses of Parliament would need to confirm the order by affirmative resolution before it became law. A Bill was introduced to implement these recommendations. The code-making power was passed into law, but the power in the Secretary of State to make orders was withdrawn from the Bill as a result of public outcry condemning the new powers as a dangerous threat to privacy.[18] The Information Commissioner released a draft code on information sharing for consultation in October 2010.

24. In **Canada** the federal legislation contains no specific provision relating to information sharing, although there is a broad power in a government institution to disclose personal information for a purpose where the public interest in disclosure clearly outweighs any invasion of privacy, or disclosure would clearly benefit the individual concerned. In New Brunswick the legislation provides that a public body may disclose information for any one of 24 specific, narrow purposes.[19] Both Alberta and British Columbia permit disclosure in a range of narrowly defined circumstances, but also where the information is necessary for the performance of the duties of an officer or employee of a public body, or where disclosure is necessary for the delivery of a "common or integrated" programme or service.[20] We return later to this concept, which we think holds promise.

25. In **Australia**,[21] the government has adopted a non-legislative National Government Information Sharing Strategy (NGISS). It emphasises the importance of a culture of collaboration, but also the need to take privacy into account. The Privacy Act 1988 (Cth) also empowers the Privacy Commissioner to make public interest determinations (PIDs), which might allow sharing in particular circumstances: these lie somewhere

---

17 Thomas & Walport, above n 8, at 3.

18 The UK position is more fully discussed in Law Commission, above n 2, at [10.71]–[10.87].

19 Right to Information and Protection of Privacy Act RSNB 2009 c R-10.6, s 46.

20 Right to Information and Protection of Privacy Act RSA 2000 c F-25, s 40(1); Freedom of Information and Protection of Privacy Act RSBC 1996 c 165, s 33.2.

21 More detailed discussion of the position in Australia is contained in Law Commission, above n 2, at [10.97]–[10.113].

between codes of practice and section 54 exemptions under the New Zealand Privacy Act. The Commissioner must be satisfied that the public interest in engaging in the practice outweighs to a substantial degree the public interest in adhering to the privacy principles.

26. In New South Wales the Privacy Commissioner may, with the approval of the relevant minister, make a direction exempting an agency from complying with a privacy principle: this power has been used to enable agencies to exchange personal information. Similar exempting powers are available in the Northern Territory, Queensland and Tasmania: in each case an exemption can only be granted if the public interest outweighs the individual interest in privacy.

27. In **Ireland** in 2008 a report on transforming public services noted the need for legislative change to facilitate information sharing. To date there appears to have been no action.[22]

THE PRINCIPLES FOR REFORM

28. In our Issues Paper[23] we suggested five principles to guide reform. They are based on similar principles contained in a 2008 UK report.[24] There was general agreement with them on the part of submitters to our Issues Paper. In summary they are:

(a) Information sharing initiatives should be judged on a case-by-case basis. It is not a case of "one size fits all". Each sharing programme is different.

(b) There should be proportionality. The extent of the sharing should be neither greater nor lesser than necessary to meet the purpose. One should not use a sledgehammer to crack a nut.

(c) The risks of sharing must be managed, in particular the risks to individual privacy.

(d) Agencies must be held accountable if something goes wrong.

(e) There must be transparency, so that people know what is happening to their information. It is destructive of trust if information gets into other hands or is used for purposes that the individual did not know about.

---

22 Law Commission, above n 2, at [10.114]–[10.115].

23 Law Commission, above n 2, at [10.116]–[10.123].

24 Thomas & Walport, above n 8.

SOME OPTIONS CONSIDERED

29. In our Issues Paper we put forward a number of options for reform. The reaction to them, and discussion of them, by submitters on the Issues Paper have enabled us to dismiss a number of the options from further consideration. We briefly summarise the most significant of those options and our conclusions about them after considering the submissions and the views expressed in subsequent consultations.

Options not requiring amendment to the Privacy Act

30. **First**, a set of guidelines, whether prepared by the Office of the Privacy Commissioner (OPC), or by another agency in consultation with OPC, as to what is now possible under the Privacy Act principles would be very helpful.[25] However we think that guidelines on the present operation of the principles are not enough alone. As we have said, every sharing programme is different. Guidelines must of necessity be at a fairly high level of generality and may not resolve some of the uncertainties about particular arrangements. Nor can guidelines vary the information privacy principles. So we believe that something more than guidelines is necessary. We do not wish, however, to be taken as undervaluing guidelines. If our recommended option is accepted, we would expect that guidelines would be prepared to assist in its operation. They might be prepared by OPC, but it might be just as valuable for them to be prepared by a cross-agency group.

31. **Secondly**, another possibility put forward in the Issues Paper was the formulation and publication of a government national strategy on information sharing.[26] This is subject to much the same reservation as the guidelines solution. Such a strategy would operate at a high level of generality, and it is hard to see how it could give the specific guidance needed for individual programmes. Nor could a non-legislated strategy change the law.

32. **Thirdly**, a Code of Practice relating to sharing made by the Privacy Commissioner under her statutory powers[27] remains a possible option, but a general sharing code would (again) have to be at a high level of generality, so it would probably be necessary to formulate a number of specific codes for particular sharing activities. The

---

25 Law Commission, above n 2, at [10.128]–[10.132].

26 Ibid, at [10.136]–[10.140].

27 Ibid, at [10.133]–[10.135].

principle that sharing should be assessed on a case-by-case basis militates against the formulation of codes for "categories" of sharing. Even a code for the "welfare" sector might be too wide (what exactly constitutes "welfare"?).[28] The preparation of codes is resource intensive. OPC has to date not favoured this solution. So we do not put codes forward as a best option, although they remain a possible one.

33. **Fourthly**, the Privacy Commissioner has power under section 54 of the Privacy Act to grant exemptions, or waivers, from the principles.[29] It would in theory be possible to "authorise" particular sharing programmes in this way. However there was very little support for this option. Section 54 is focussed on "one-off" exemptions rather than continuing programmes. Moreover, its use in this new context would effectively amount to a substitution of new rules rather than an exemption, and would not be very different from the code-making power.

Options requiring amendment to the Privacy Act

34. **First**, it may be possible to improve the current situation by making minor amendments to some of the exceptions to the principles. One that commands considerable support is to remove the word "imminent" from the exception to principles 10 and 11 which allows use or disclosure when that is:[30]

> necessary to prevent or lessen a serious and imminent threat to –
>
> (i) public health or public safety; or
>
> (ii) the life or health of the individual concerned or another individual.

A threat can be serious, and thus require preventing or lessening, even though it is not likely to eventuate on the instant. The Commission is likely to recommend such an amendment in its Report on the Review of the Privacy Act. The amendment would delete the word "imminent", and provide that in determining whether a threat is "serious", regard should be had to such matters as the likelihood that it will eventuate, the nature of the consequences if it does eventuate, and the time at which it may eventuate. In that way, imminence would not be a necessary condition, but simply one matter to be taken into account. Obviously, however, such a specific amendment would solve only a small part of the problem.

35. **Secondly**, we also floated in the Issues Paper the idea of including a "welfare"

---

28 See para [35] below.

29 Law Commission, above n 2, at [4.92]–[4.97].

30 Ibid, at [10.190]; Privacy Act 1993, s 6.

exception.[31] It might be added to the existing health and safety exception to cover a threat to "health, safety or welfare". There is precedent in Victorian legislation, and in a Bill in Western Australia.[32] While there was a little support for this in submissions, there was opposition too. We do not favour this option. "Welfare" is altogether too vague. It can mean different things to different people. Moreover, what is to one person's welfare may be to another's disadvantage. If one extended it to include the welfare of society as a whole in addition to the welfare of an individual, as some would like, all shape would be lost. Such an exception would open the door far too wide. It would be extremely difficult to police it.

36. **Thirdly**, another option put forward in the Issues Paper was a "public sector as a single agency" provision.[33] It was presented in the form of a general presumption that information supplied to one agency can be disclosed to other agencies to achieve a purpose which is beneficial to the individual and is broadly similar to the purpose for which the information was collected or obtained. This received a mixed reception in submissions. We think it is too ill-defined, and consequently do not support it. What is a "broadly similar" purpose? When can it be said that a purpose is "beneficial to the individual"? We felt such a provision could generate fear that personal information provided to one agency would automatically be available across the board to other agencies: public confidence would not be enhanced by such a provision. We have emphasised the importance of trust: this kind of provision could do considerable damage to trust.

37. **Fourthly**, we also presented an option of amending the Act to allow the Privacy Commissioner to make binding rulings that programmes meet, or do not meet, the requirements of the Privacy Act.[34] This option attracted very little support. There were concerns about its relationship with the complaints process. Moreover privacy cases are very fact-specific and it may not be appropriate for rulings on one set of facts to be binding on others. Furthermore, such a solution could do no more than validate activities that were already Privacy Act compliant. We are not pursuing this option.

THREE PRELIMINARY POINTS

31 Law Commission, above n 2, at [10.190]–[10.191].

32 Discussed in Law Commission, above n 2, at [10.190]–[10.191] and also at [10.113].

33 Ibid, at [10.141]–[10.148].

34 Ibid, at [10.149]–[10.174].

38. Before proceeding to discuss our preferred option, we would re-emphasise three points. First, whatever solution is adopted there will always remain room for guidance, from OPC as well as other agencies. There is already much valuable guidance on OPC's website: it is one of OPC's statutory functions to provide it. Guidance is not law and does not have binding force. No doubt whatever solution is finally provided for the problem of sharing, OPC guidelines can enhance it, and the understanding of it, just as it can clarify what is allowed under the existing principles and the exceptions to them. Secondly, in our report on the Privacy Act we shall be examining in detail the question of whether some of the existing principles and the exceptions to them need refinement. We noted in paragraph 34 the amendment to the "health and safety" exception that we are likely to recommend. Such amendments of detail could take place in addition to our preferred option. Thirdly, law reform alone will not solve all the problems which are currently apparent. Changes in culture and organisation will also be required. But we believe law reform is a necessary condition.

PREFERRED OPTION: THE APPROVED SHARING PROGRAMME

39. We now discuss the option that we prefer. It is in fact an amalgam of two of the options set out in the Issues Paper, both of which received substantial support from submitters.[35] We have also presented the idea at a number of forums and round-table discussions with agencies. It received significant support in principle on those occasions.

40. We believe that the greatest promise is held by the concept of an "approved sharing programme". In two Canadian provinces, Alberta and British Columbia, one of the statutory exceptions to the non-disclosure principle is "a common or integrated programme or service".[36] In neither Act is this phrase defined; instead its meaning is spelt out in guidance. The detail is, as it were, below the surface. Examples given in the Alberta guidelines suggest that the concept is principally focussed on programmes of beneficial service of the Linwood Service Centre kind.[37]

41. We think that for New Zealand the Canadian concept should be extended in two ways. First, we think that the exception should cover all types of sharing programmes and not

---

35 Ibid, at [10.198]–[10.203] and [10.208]–[10.221].

36 Ibid, at [10.89]–[10.96], discussing Right to Information and Protection of Privacy Act RSA 2000 c F-25 and Freedom of Information and Protection of Privacy Act RSBC 1996 c 165.

37 Access and Privacy Service Alberta "Common or Integrated Programmes or Services" (March 2009) *foip bulletin* 8

just "beneficial service" programmes. In fact we think it would be quite difficult to isolate such a category. The solution we propose would be a general one which would cover programmes whose sole purpose is to provide holistic service to an individual or family; programmes which envisage the taking of adverse action against an individual; programmes which combine both these things; and programmes which raise at least the possibility that both may be involved. It would also include programmes which are presently dealt with as information matching. In other words, the concept should be the broad one of an "approved information sharing programme". Secondly, we believe that such programmes should require formal approval by Order in Council, and that legislation should lay down explicit rules for that approval, and clearly prescribe the protections which surround such programmes. Only in this way can the risks that attach to sharing programmes be sufficiently managed and solutions to them be prescribed. The types of programme are likely to vary considerably. Some would involve more agencies, more information, and more risks than others. Some might modify the application of one or more of the information privacy principles in the Privacy Act. The safeguards and checks and balances would need to be proportionate to those varying levels of risk.

42. In essence what we are proposing is a system whereby agencies proposing a sharing arrangement would draw up an agreement (or protocol); that agreement would be subject to an approval process culminating in approval by Order in Council; and the approved programme would be publicly notified and included in a schedule to the Privacy Act. By that process agencies can have certainty, and can demonstrate to the public that what they are doing is permitted by law even though there might otherwise have been an argument that the principles in the Privacy Act did not cover the activity. There will also be an assurance that threats to privacy have been identified and appropriately managed.

43. We believe that the new machinery should be contained in a separate part of the Privacy Act dealing with the sharing of personal information between government agencies. We do not favour the solution of a separate "Information Sharing" Act. That way the privacy implications could too easily be forgotten. The Privacy Commissioner will have an important role to play, and the new provisions should be in the same Act that lays down the Commissioner's functions. Moreover, the provisions about information matching, which we see as a special form of sharing, are currently located in the Privacy Act.

44. The legislative provisions would deal with the following matters. In formulating these criteria we have worked from first principles, but have also been guided by the current rules about information matching (suitably adapted to the less formal context) and the proposed provisions of a Bill currently before Parliament.[38]

Approval

45. There should be a statutorily prescribed process for establishing sharing programmes. The two or more agencies involved would prepare a written agreement containing the details of the proposed sharing programme. In preparing it they would be required to consult with appropriate persons and agencies: OPC would be able to recommend, and the relevant ministers to require, that certain persons be included in the consultation. Some programmes would obviously require more consultation than others. Consultation with OPC would be mandatory. In the case of more extensive programmes OPC might require that a privacy impact assessment be undertaken.

46. The programme would then be signed off by the relevant portfolio ministers and would be submitted to Cabinet for approval. A report from OPC would be considered by Cabinet as part of the approval process; that OPC report should be a public document.

47. The criteria for approval should be:

- That the purpose of the programme is to achieve a significant benefit to society or to individuals. "Benefit" may include, but is not confined to, economic benefit.
- That the benefit to be achieved by the programme outweighs the risks involved, in particular the risks to individual privacy.
- That the type and quantity of information to be shared, and the number of agencies involved, are necessary for the attainment of the purpose of the programme.
- That the safeguards contained in the programme agreement are adequate and proportionate to the risks involved.
- That the programme agreement provides for the matters prescribed by the Act.

Before approving a programme Cabinet would be required to take into account:

- The degree to which the proposed programme departs from the information privacy principles in the Privacy Act.
- Whether there are other ways of achieving the desired purpose, and whether the

[38] See the Privacy Act 1993, Part 10 and sch 4; also the Customs and Excise (Joint Border Management Information Sharing and Other Matters) Amendment Bill 2010 (200-2), cl 25 adding new s 286A to the principal Act.

proposed programme is the best way (the agencies involved would need, in other words, to explain the options they had considered).

- The results of the consultation process and any recommendations of OPC.

Contents of agreement

48. The Act should provide that the agreement between the agencies must contain the following:

    - A clear statement of the purpose of the programme.
    - A clear statement of the category or categories of personal information which may be shared. (These should be stated with some specificity. It will not be enough to provide for open-ended ill-defined categories of information.)
    - A list by name of the agencies participating in the programme and the types of information to which each is entitled. Not all agencies might necessarily be entitled to all types of information. There should be provision that if agencies later change their names, or if their functions are transferred to other agencies, the list in the agreement will be read as referring to the up-to-date version.
    - A clear statement of the uses to which a recipient agency may put the information.
    - A requirement to establish and maintain detailed technical standards.
    - A description of the safeguards to be adopted to ensure security of the information shared. The more sensitive the information the higher will be the required level of security.
    - Details of how the general requirements of the Privacy Act relating to sharing programmes are to be met.
    - The nomination of one agency as the lead agency (to prevent confusion about responsibility for such things as reporting).

49. It may be possible for model template sharing agreements to be prepared – perhaps by OPC or the State Services Commission – to serve as a guide. However any template would need to be modified for the purpose of an individual programme; we recall the principle that sharing activities must be assessed on a case-by-case basis. We would also expect guidance to be available as to the appropriate level of safeguards for various categories of agreement.

General rules applying to all programmes

50. The Act should also contain some mandatory general requirements which would apply to all sharing programmes.[39] It should provide as follows:

(a) Safeguards

(i) Information subject to a sharing programme may only be used by, or disclosed to, agencies participating in the programme and for the purposes stated in the programme. However, there would need to be an exception to this to deal with exceptional situations where either the health and safety or maintenance of the law exception required it. Information could then be disclosed to the agency appropriate to deal with it.

(ii) If as a result of an information sharing programme information is discovered that results in the need to take adverse action against an individual, the individual must be given a period of notice and an opportunity to object to the proposed action. Adverse action would be defined as in the current matching provisions of the Privacy Act[40], but with the addition of a decision to impose a penalty and a decision to recover a penalty or fine earlier imposed. The period of notice should be at least ten days, although with power in the Privacy Commissioner to approve a lesser period in particular circumstances. There would need also to be an exception to the requirement of notice if action is urgently required as it might be, for example, in a case of child abuse or domestic violence. The time limit for commencing adverse action should be 12 months, as it currently is for information matching.[41]

(iii) Information obtained by an agency in the course of an information sharing programme must not be kept for longer than necessary for the purposes of the programme.

(b) Transparency

The Privacy Act is itself based on the premise that individuals have a right to know what information is held about them, and the purposes for which it is being used. The proposed legislation should expand on the application of those principles to sharing arrangements. It should provide as follows:

---

39 Again, some of these requirements have been adapted from the current matching provisions.

40 Privacy Act 1993, s 97.

41 Privacy Act 1993, s 101(2).

(i) Agencies involved in a sharing programme must take all reasonable and practicable steps to ensure that the individuals subject to the programme are notified of it.

(ii) The text of an approved programme agreement must be published on the website of the lead agency, with links on the websites of the other participating agencies. Individuals who are, or could be, affected will then know which agencies may hold their information, and can if they wish exercise their right under principle 6 of the Privacy Act to have access to it.

(iii) The lead agency must report annually on the operation of the programme. In most cases it would be enough to have this report as one part of the agency's annual report, but in appropriate instances it might be made a condition of the initial approval of the programme that the report be made to OPC as well. If concerns later develop about the operation of a programme OPC should also be able to request a report to them.

(iv) On the approval of each programme it should be added by Order in Council to a schedule of the Privacy Act. In this way the number and nature of all existing programmes could be seen at a glance. Ideally the schedule would follow much the same form as the present Schedule 5 (the Law Enforcement schedule) and would indicate the agencies involved, the type of information shared, and the purpose of the sharing. Such a schedule would provide information for the public, and ready assurance for agencies and others that what the agencies are doing is permitted by law. In a sense this power to add to a schedule by Order in Council may look like what is sometimes called a Henry VIII clause.[42] But the purpose of such additions to the schedule would just be to provide *information*: they would record the result of a statutorily authorized process. In that sense the procedure is no more exceptional than several other provisions which allow statutory amendment by Order in Council.[43]

(c) Accountability

A breach of any of the provisions of the Act relating to sharing programmes and/or a breach of any of the terms of an approved programme would, provided the statutory

---

42 See Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (May 2001) at [10.1.8].

43 See for example Misuse of Drugs Act 1975, s 4. Compare Education Act 1989, s 162(2), which enables the Governor-General by Order in Council to establish new universities without the need even to add them to the list of existing universities in schedule 13.

harm threshold was reached, constitute an interference with privacy and thus be a ground of complaint to the Office of the Privacy Commissioner. The Act would need to make express provision to this effect. Currently the Commissioner attempts to resolve complaints by a process of mediation or negotiation. Those which cannot be resolved in this way may proceed to the Human Rights Review Tribunal. In our forthcoming report on the review of the Privacy Act we shall investigate whether the Privacy Commissioner should have greater powers to enforce compliance.

(d) Parliamentary oversight

Parliamentary enactment for each sharing programme is not envisaged, but it is desirable that the process be subject to parliamentary oversight. The Orders in Council approving programmes should be disallowable instruments under the Regulations (Disallowance) Act 1989. They would be subject to the scrutiny of the Regulations Review Committee. That committee would apply the grounds in Standing Orders for drawing a regulation to the attention of the House, among them that it trespasses unduly on personal rights and liberties, or that it makes unusual or unexpected use of the statutory powers.

(e) Review

For resource reasons we do not suggest that programmes be subject to mandatory review after any set period of years, but if any annual report, or other evidence, indicated that a particular programme was not working satisfactorily, or that it was no longer required, or that its purpose had changed, OPC could initiate a review of it. (Such a review might indicate that the programme should be formally amended.) On the other hand, we do think that the new statutory framework we are proposing should be reviewed after the first three years. Given the speed of developments in technology, and the importance of information sharing for both individuals and society, it is desirable that the operation of the new process be examined to ensure that it remains fit for purpose. There should be provision in the Act for such a review by a person or body nominated by the Minister. OPC should be centrally involved in such a review.

DISCUSSION

51. In our view this proposal satisfies the five principles we have outlined in paragraph 28

above. In some cases the sharing provided for in an approved programme might be permissible already under the principles in the Privacy Act and the exceptions to them. In such a case the approval of the programme would give the participating agencies a confidence and certainty they may not have had previously. On the other hand, in other cases the activities might, arguably, not be protected under the Privacy Act as it currently stands. In that case the approved programme would validate sharing that might otherwise have been open to question.

52. The essential feature of the proposal is the approval of each individual sharing programme by Order in Council. There may be some who believe that sharing programmes involve such significant risk that they should be specifically authorised only by Act of Parliament, as is effectively the case now with matching programmes. It might be argued that given the potential threat to individual rights specific authorisation by Parliament itself is more appropriate. However we think Order in Council is the preferable vehicle. Parliamentary time is a scarce resource, and the delays involved in getting the appropriate Bill on the Parliamentary agenda and in getting the Bill passed would be highly undesirable. Provided the Privacy Act itself contains carefully formulated rules of the kind we have outlined the safeguards should be adequate. They include the consultation process; the involvement of OPC and the publicity of the OPC report; the transparency requirements; and the possibility of disallowance. Given that Cabinet processes are not as open as Parliament's, it is clear that there need to be such safeguards.

53. Nor is the Order in Council route contrary to the general scheme of the Privacy Act. Although the Act does currently provide for the statutory creation of matching programmes and also the statutory addition of items to Schedule 5, it also confers very considerable power on the Privacy Commissioner to make delegated legislation in the form of codes, albeit subject to a prescribed consultation process. Those codes can vary the statutory privacy principles. To authorise the approval of sharing programmes by the Order in Council process is not, it seems to us, out of place in that statutory context.

54. However this is not to exclude the possibility that there may be situations where special far-reaching measures are necessary, and where special legislation may be the most appropriate vehicle. An example might be a situation where it is felt necessary to impose enforceable *duties* to disclose information to protect a particular category of vulnerable person.

55. On the other hand, there may be some who view the Order in Council process as overly bureaucratic. Some might prefer a more streamlined procedure. We agree that there should not be unnecessary bureaucracy, and that the imposition of burdensome procedural hurdles would deter agencies. But we do not think that what we propose creates unreasonable burdens. One would hope that any sharing arrangement would even now be accompanied by a careful written protocol, and that the Privacy Commissioner would be consulted. One would also hope that risks were properly managed. A Chief Executive should properly insist on that. The suggested procedure only ensures that this will happen, and involves the further step of Cabinet approval to ensure independent scrutiny. The requirement of transparency is also no more than good practice should already require. Transparency is a basic tenet of the information privacy principles.

TWO CURRENT ARRANGEMENTS

56. At present the Privacy Act makes provision for two activities which are effectively types of information sharing: these are information matching and access to law enforcement information. The question is how these two existing sorts of arrangement will fit with the proposed regime for information sharing.

Information matching

57. We have carefully considered the matter of information matching. That is currently the subject of a statutory regime which has been in the Privacy Act from the beginning.[44] Matching programmes are individually authorised by specific provisions in Acts of Parliament. OPC has the function of assessing proposals for such statutory authorities against a set of guidelines contained in the Privacy Act.[45] Once a matching programme has been approved by its own separate Act of Parliament, a reference to that Act is added to a schedule to the Privacy Act (Schedule 3) and must be operated according to matching agreements approved by OPC; these agreements must comply with a set of rules contained in the Privacy Act.

58. It is our view that, provided adequate safeguards are included in the Privacy Act, it is best to treat information matching as a kind of sharing, and subject it to the same Order

---

[44] Indeed it predates the Privacy Act 1993, being first enacted in the Privacy Commissioner Act 1991, and then carried forward into the 1993 Act.

[45] Privacy Act 1993, Part 10.

in Council regime as the other types of sharing. There is considerable uncertainty at the moment as to how matching is to be properly defined and as to how, if at all, it differs from sharing. The Privacy Act has two definitions of matching which at first sight bear little resemblance to each other.[46] They are the cause of considerable confusion. An **authorised information matching programme** means:

> the comparison (whether manually or by means of any electronic or other device) of authorised information matching information with other personal information for the purpose of producing or verifying information about an identifiable individual.

On the other hand an **information matching programme** means:

> the comparison (whether manually or by means of any electronic or other device) of any document that contains personal information about 10 or more individuals with one or more other documents which contain personal information about 10 or more individuals for the purpose of producing or verifying information which may be used for the purpose of taking adverse action against an identifiable individual.

There is no internationally accepted definition of matching. A recent guide prepared by the Victorian Privacy Commissioner for the Victorian public sector says:[47]

> Although in common use the term "data matching" means different things to different people. No standard definition exists. Various activities involving the comparison of separate data sets may be referred to as data matching.

59. We have considered the possibility of ring-fencing a narrow type of matching within a precise definition and retaining the current Part 10 of the Privacy Act to deal with it. One might, for example, use the second and narrower "two sets of 10 persons" definition cited above. However, this would be artificially narrow and entirely arbitrary. There would be no point in it. The risks involved in this kind of "bulk matching" activity do not seem to be any greater than those involved in collating information about a known individual from a number of separate databases.

60. So we prefer to treat matching simply as one type of sharing, and to apply the same Order in Council process for programme approvals. The safeguards would, we believe, be just as effective as those currently applied. In fact a good number of the provisions we have recommended for sharing programmes are modelled on the Act's current matching regime.

61. There will be a question as to what happens to matching arrangements which were in force before the change. We believe they should simply be grandparented without any

---

46 Privacy Act 1993, s 97.

47 Privacy Commissioner *Data matching in the Public Interest: a Guide for the Victorian Public Sector* (August 2009) <www.privacy.vic.au/privacy/web.nsf>.

need to be re-approved, but in relation to their ongoing operation they should be subject to the new rules.

Schedule 5

62. Schedule 5 of the Privacy Act contains a list of agencies which can share law enforcement information, and the types of information which can be shared. In the early years the schedule could be added to by Order in Council, but now that is done by Act of Parliament.

63. The question is whether law enforcement is sufficiently distinct to have its own regime under schedule 5. We think not. While law enforcement information is sensitive, so are other types of information which we would envisage being included in sharing arrangements (for instance, child welfare and financial information). Also, any exclusive regime for law enforcement could lead to confusion and difficulty in cases where a sharing arrangement involved both law enforcement information and other types of information.

64. We therefore propose that the new information sharing regime should encompass law enforcement information, and that there should no longer be a separate schedule 5. The arrangements in the present schedule 5 should be grandparented and transferred to the general information sharing schedule. New law enforcement arrangements should be subject to the new approval rules.

SCOPE

Types of programme

65. It would be totally unrealistic to require that all disclosure of personal information between government agencies must take place in accordance with a programme approved in the way, and by the process, that we have outlined. Sometimes it may be acceptable, even necessary, for one agency to supply information about an identified person to another so long as such supply is in accord with the Privacy Act's principles. If, for example, a dangerous psychiatric patient has escaped from confinement it would be absurd to suppose that the Ministry of Health could not immediately liaise with the Police. Ad hoc sharing of this kind, which is within the Privacy Act principles, must be allowable. Indeed, it does not involve a "programme" at all.

66. What we are concerned with in this paper is continuing *programmes* or *arrangements*

for sharing which involve categories of information and groups of as yet unidentified individuals.

67. There are two options. **One** is that all such programmes should require formal approval. The basis for this would be that government agencies are in a unique relationship with their citizens where trust is particularly important, so that if they engage in the activity of sharing citizens' information they should get approval for it. All programmes would then be on the same basis, subject to the same checks and balances, and equally transparent.

68. The **second** option is that programme approval is only required if the programme is not compliant with the Privacy Act principles and their exceptions. This would, in a sense, give the agencies some discretion. They *might* decide to apply for approval even if the programme were Privacy Act-compliant; they would *have* to do so if it were not compliant; and would be strongly *advised* to do so if there was uncertainty or disagreement about whether it was compliant or not.

69. It should be noted that currently it appears to be possible to match information without going through the process set out in Part 10 of the Act: there is no provision in the Privacy Act explicitly saying that information matching requires statutory authorisation. Nor is schedule 5 the only avenue for accessing law enforcement information: it may sometimes be possible by simply relying on the "maintenance of the law" exception to the disclosure principle.

70. Of these options, we prefer the first. There would be some discomfort about having two sets of programmes, one approved and the other non-approved. It might engender unjustified suspicion of the non-approved. Moreover, agencies might wrongly assume that their programme was Privacy Act-compliant when in fact it was not, and thus fail to seek approval. The second option would also mean that the list of approved programmes in the schedule did not tell the whole story.

71. Yet, we acknowledge that the approval process will involve resources, and to require approval of all programmes would involve more resources than the second option. That would be so not just for agencies, but also for OPC, although it is not clear just how much greater the burden on OPC would be: it already spends a lot of time answering agency queries about the subject, and is heavily involved in all matching programmes. There is also something anomalous about requiring a formal process to be gone through in relation to activities which have been going on, perhaps for years, in full compliance with the Privacy Act.

72. So while we prefer the first option we would not oppose the second. But if the second is chosen, we believe that transparency should still be required. The agencies engaging in non-approved programmes should therefore be required to publicise them on their websites, and report on them annually. It would also be desirable for a list of such arrangements to be compiled and published on the internet by either the Ministry of Justice, or the State Services Commission, or the Office of the Privacy Commissioner.

Agencies

73. A further question is whether the new sharing programme rules should apply only to sharing between central government agencies or whether they should also include the private sector, non-governmental organisations (NGOs) and local government. This question is likely to be raised increasingly frequently in this new age where there is increasing talk about public-private partnerships. We note that the current matching rules in the Act apply only to "public sector agencies".

74. We are nervous about extending the approval processes that we are recommending to NGOs. For one thing, much work needs to be done in determining the preparedness and capacity of some NGOs to participate in sharing programmes, particularly in relation to their technical capacity. Moreover the question of trust is a particular issue in relation to NGOs. Many NGOs are charities that receive information from individuals in confidence. If an individual entrusts personal information to, say, the Salvation Army or the Plunket Society, he or she usually does not expect it to end up in the hands of a government department. We have discussed proposals for sharing programmes with a group of NGOs and, while their reactions differed, it was clear that some of them harboured considerable concern about this.

75. However, we understand that some "beneficial service" programmes do benefit from the involvement of NGOs and that in such cases the information the subject of the programme is usually supplied *to* the NGOs rather than being received *from* them. Provided a particular NGO can satisfy the security requirements – a matter for the programme approval process – we think it could become part of a sharing arrangement on the limited basis that we have indicated in this paragraph.

76. There may be cases, too, where it is proposed that an NGO should act solely as an *agent* for the government agency. In such a case it would be just as if the government agency was doing the job itself. This might also be acceptable, provided a provision in the Act made it clear that information in the hands of the NGO was deemed still to be

held by the government agency, which remained responsible for the information, and accountable for anything that happened to it. It would be necessary to adapt the present section 3(4) of the Privacy Act to the purpose, or insert a new provision to similar effect.

77. With regard to the private sector and local authorities, however, we think that the proposed sharing programme process should be allowed time to bed in within the central government agencies before extending it thus far beyond them. It is often best to introduce new concepts and processes with caution, and not to open the door too wide from the outset.

78. Should the proposed system be adopted and come into being, it would still be possible to pass individual Acts of Parliament to authorise exceptional arrangements which go beyond what is currently proposed. Parliament is sovereign. There may be exceptional public-private partnerships which would justify such a solution. When the new system has been operating for a sufficient time for it to be possible to assess its operation, the general legislative framework here proposed could be amended to include additional classes of agency.

79. So our present view is that, with the limited exception for NGOs which we have outlined, the new sharing provisions should initially only apply to Ministers, departments and other organs of central government.

PROPOSALS

We thus propose:

(1) That the Privacy Act 1993 should be amended to make provision for the approval of programmes for the sharing of personal information between government agencies.

(2) That such programmes should require approval by Order in Council.

(3) That the Privacy Act should expressly lay down the process of approval, which would involve consultation with appropriate persons including the Privacy Commissioner; the criteria for approval; the matters required to be contained in programme agreements; and general rules for the operation of such programmes. The general rules should provide safeguards, require transparency, and provide for means of accountability.

(4) That Orders in Council approving programmes should be disallowable instruments within the Regulations (Disallowance) Act 1989.

(5) That information matching should be treated as a form of information sharing, and be subject to the same processes and rules. Existing matching programmes should not have to be re-approved, but in their ongoing operation they should be subject to the new rules. The same should be true of law enforcement information currently contained in

schedule 5 of the Privacy Act.

(6) That the proposed regime should apply to all continuing programmes of information sharing between government agencies. If, however, it is decided that approval should be required only for programmes which are not otherwise compliant with the Privacy Act, the transparency requirements should apply to the non-approved programmes.

(7) That, in the first instance, the proposed regime should apply only to sharing between central government agencies, although in appropriate cases it might be extended to include non-governmental organisations on the basis described in paragraphs [75] and [76].

(8) That all approved programmes should be listed in a schedule to the Privacy Act 1993.