Office of the Inspector-General of Intelligence and Security

2016-17 Review of NZSIS requests made without warrants to financial service providers
REPORT

Cheryl Gwyn
Inspector-General of Intelligence and Security
26 November 2018

1. Both of the agencies I oversee, the New Zealand Security Intelligence Service (NZSIS or the Service) and the Government Communications Service Bureau (GCSB), obtain information from third party agencies on a voluntary basis. In this report I refer to that process as "voluntary disclosure." The voluntary disclosure process is lawful, subject to the principles I discuss in this report. This public report sets out a summary of my findings about the NZSIS's practices in 2016/17 in seeking voluntary disclosure from banks. The timeframe of my review means that the new Intelligence and Security Act 2017 (ISA) was not in force at the time, but I have taken the opportunity to note principles and issues that will also be relevant to lawful operational practice of this type under the new Act. Much of my full report is classified, and this version is necessarily a summary of the key points. The recommendations are as I provided them to the NZSIS.

2. When making a voluntary disclosure the external agency is not responding to an enforceable power, such as an intelligence warrant,[1] and the provision of information in response to a request is voluntary. Where the external agency provides services directly to customers, as banks do, there is a high chance that information sought by the intelligence and security agencies to further an investigation will be "personal information" in which the customer has a reasonable expectation of privacy. Because the information in question is not gathered by the external agencies for the purposes or benefit of intelligence agencies, it is necessary to ensure that any State access mechanisms are lawful, robust, and proportionate. Regular review, active oversight and agency accountability are particularly important where NZSIS and GCSB source personal information from external agencies without a warrant or other lawful authorisation.

3. Over the last year or so there has been increased attention given to the restraints and responsibilities on State agencies making voluntary requests of this type. It is clear that when a State agency makes requests of service providers for customer information, the right of individuals to be free from unreasonable search and seizure in s 21 of the New Zealand Bill of Rights Act 1990 (BORA) applies.[2]

4. The NZSIS has historically made frequent requests to banks and other financial services agencies for voluntary disclosure of information.[3] The information it sought related to the Service's broad functions in respect of matters relevant to New Zealand security, and generally concerned persons of intelligence interest. In 2016 I decided to review this area of its practice, in part because it was an activity outside the parameters of supervision provided by any warrant. While many of the same issues arise with respect to other public or private third party agencies who receive requests from the Service for voluntary disclosure of people's private information, personal banking information is predictably likely to contain especially

---

1 An intelligence warrant is necessary for activities that would, in the absence of authorisation, be unlawful. Warrants are issued by the Minister responsible for the intelligence agencies, and, if they relate to a New Zealander, also by the Commissioner of Intelligence Warrants. See Part 4 of the Intelligence and Security Act 2017.

2 *R v Alsford* [2017] 1 NZLR 710 (SC); and also https://www.privacy.org.nz/blog/hager-and-westpac/ The full text of the Police acknowledgement and apology to Mr Hager can be found at www.scoop.co.nz/stories/PO1806/S00109/police-apologise-to-nicky-hager.htm.

3 In this report I use the term "banks" to include non-bank financial institutions where these institutions provide a similar service to the public as banks.

personal, confidential, and sensitive information. The frequency of the Service's use of this mechanism, the fact it was not specifically and independently authorised, and the nature of the information sought, made focussing on voluntary disclosure from banks an obvious area to review.

5. Data held by banks on their customers is substantial. It can disclose an individual's pattern of life and can go to what is sometimes called a person's 'biographical core.' Beyond specific financial details (eg the account balance at a point in time; or the recipient of specific fund transfers and payments) banking data may encompass or reflect information such as a person's movements, their day to day activities, their personal relationships, employment history, major health issues, and their current and past contacts.

6. The review and my consequent report were slowed in the final stage by the enactment last year of the ISA. Specific provisions for the intelligence and security agencies to obtain business records were incorporated in the ISA, largely as a result of concerns expressed by telecommunications companies and banks at their perceived legal vulnerability when faced with requests for voluntary disclosure.[4] I considered I should use the opportunity of this review to also ensure that there would be improved practices in place to reflect the Service's obligations under the ISA. Accordingly, while my review only examined the particular practices and policies in place prior to the ISA, my findings are relevant to how the Service should implement and approach its powers and responsibilities under the new legislative regime.

7. I have had open and constructive discussions with the NZSIS about all of the matters covered by this report, and it is to the Service's credit that it has been willing to reconsider its position on certain matters, discuss developing policies, and make changes to many of its processes, as this review and report have progressed. I have made three recommendations at the end of this report, and the Service has responded to each of them. With regard to recommendation 1, it has created an accessible database of all requests made to financial institutions including under s 121 ISA. It has made substantial progress in implementing recommendations 2 and 3. I will continue to monitor progress against each of my recommendations. As part of my existing work programme I have also signaled I will conduct a focused review of how the Service has implemented the Business Records regime under ISA. What is already apparent is that a good deal of work has gone into preparing the relevant internal policy materials, and the improvements in terms of the legal issues I have discussed in this report are already visible.

Voluntary disclosure principles

8. The general principles governing State requests for voluntary disclosure will apply to requests made to almost all third party agencies. In one respect, however, financial institutions are in a

[4] The New Zealand Bankers' Association in its submission (7 Oct 2016) to the Foreign Affairs, Defence and Trade Select Committee on the New Zealand Intelligence and Security Bill indicated that its members felt legally exposed when responding to non-compulsory requests for information, paragraphs 10 and 11.

special position: banks are subject to a legal duty of confidentiality which applies to all bank customer information whether significant or trivial.[5] Given what banking information can disclose about an individual's personal affairs it also predictable that, from the customer perspective, banking information will be considered to be reasonably confidential, or even "sensitive."

9. The guarantee in s 21 BORA to be free from "unreasonable search and seizure" will apply to a State request for voluntary disclosure of personal information. This is because s 21 provides a shield to protect the individual from the State's request where the individual has a "reasonable expectation of privacy" in the information at issue. If the person does have a reasonable expectation of privacy there will be a "search" for the purposes of s 21.[6]

10. New Zealand law does not require that every act constituting a "search" or every intrusion by the State into personal privacy needs to be authorised by a warrant, but intrusions that engage reasonable expectations of privacy (ie searches) are likely to be unlawful if they are not permitted by a statute or independently authorised, eg by a warrant or production order.[7] Unlawfulness arising from a lack of authorisation will also generally render a search "unreasonable," and therefore in breach of s 21 BORA.[8] Accordingly, there is a risk that a more than minimally intrusive search, without any exigent circumstances to justify failure to obtain an authorisation, is likely to be "unreasonable" and a breach of s 21 BORA.[9] Quite apart from the question of authorisation, in every case the request (or "search") must be "reasonable" having regard to factors such as the scope, content, purpose and context of the State's information request: ie is the information request itself reasonable, in all the circumstances?

11. Given these principles, requests to banks about their customers need to be carefully considered and tightly circumscribed. Most often, given that bank data will reveal details about lifestyle and personal choices, and given the common law duty of confidentiality on banks,[10] an individual will have a reasonable expectation of privacy with regard to almost all of their banking information. As a consequence, State requests for customer financial records will almost always constitute a "search." The more nuanced question is whether the search is reasonable.

12. Intrusive state action should also be consistent with the principles of necessity and proportionality. Necessity in the present context requires a compelling justification for the

---

5 *Tournier v National Provincial and Union Bank of England* [1924] 1 KC 461; and New Zealand Banking Ombudsman Casenotes, cases 40063 and 32379.

6 *Alsford* at [64].

7 For a focused discussion of the principle of legality applicable to this context see the Law Commission's recent *Review of the Search and Surveillance Act 2012* (R141, June 2017) at [4.16]–[4.24] and [14.29].

8 *R v Hamed* [2012] 2 NZLR 305 at [174] and [226].

9 *Alsford* at [64].

10 Usually reflected in a customer contract. Such contracts often have only broadly worded exceptions for disclosure: *Alsford* at [68] and [71]. Where there is reason to believe that disclosure of information is necessary for the purposes of national security that may provide an overriding exception to the bank's duty of confidentiality, or the customer's right to privacy.

request. The information does not need to be "indispensible" to the Service but it must be more than merely "useful." Proportionality concerns whether the likely value of the information to be obtained justifies the extent of the proposed intrusion on privacy.

13. A bank is obliged to reach a view on whether there is a legitimate basis to share its customers' personal information. It has long been recognised that where there is reason to believe that disclosure of information is necessary for the purposes of national security that may provide an overriding exception to the bank's duty of confidentiality, or the customer's right to privacy. The bank must also assess whether the scope of the request is reasonable. These obligations mean that the Service needs to provide the Bank with sufficient information to be able to decide for itself whether the request, and its scope, are justified.

14. My overarching conclusion from this review is that at the relevant time NZSIS did not sufficiently recognise that requests made to banks for the voluntary disclosure of customers' banking information had to be consistent with s 21 BORA. I also consider that there was at the time, and remains, very limited scope for NZSIS to make voluntary disclosure requests to banks for personal information. As a result, they should be made only where there is no, or minimal, expectation of privacy in the information. Given customers' reasonable expectations of privacy in almost all of their personal banking information, most requests for this material will constitute a "search".[11]

15. I appreciate that the Service did not at the time of my review have the benefit of the Supreme Court's conclusive decision in *Alsford*, which clarifies the point that requests of this type by the State are searches for the purposes of s 21 BORA. Nonetheless, the underlying principles are not new, and the State has always been obliged to rigorously assess and justify the extent to which it interferes with, or systematically requests others to interfere with, the privacy interests of individuals.

16. During the period in question the Service regarded s 57 of the Privacy Act 1990 (as it then was) as providing the lawful basis for its requests. This, however, was unnecessary because requests for voluntary disclosure were (and are) in principle lawful, so long as they do not breach s 21 BORA. The *Alsford* judgment has now put the role of s 57 of the Privacy Act beyond doubt. It confirmed (although not specifically dealing with s 57) that exceptions to the information privacy principles do not create any empowering provision for State agencies to request personal information from external agencies. Rather these operate as disclosure provisions enabling information-holding agencies to respond to agency requests in appropriate circumstances.[12] Section 57 would, if the legal conditions are met, provide justification and protection to banks for disclosing personal information to the Service.

---

[11] *Alsford* at [63].

[12] *Alsford* at [64] and [143], and see Privacy Commissioner's *Commentary on R v Alsford: voluntary requests for personal information by law enforcement agencies*, May 2018, p 3, at www.privacy.org.nz/news-and-publications/guidance-resources/alsford-v/

The Service's processes in 2016-2017 for voluntary disclosure requests

17. I found that there were carefully thought out and formal internal authorisation processes before a request for information was submitted by the Service to a bank. Sign-off happened at an appropriate level within the organisation. Generally there were accessible records setting out the intelligence requirements in the case, a statement of justification for the particular request, and guidance on how the requirements should be fulfilled.

18. The Service's policies directed staff to act reasonably and proportionately in carrying out operational activities. They did not, however, make clear that staff needed to assess the nature and extent of the customer's expectation of privacy in the particular information sought. I found that the Service tended to focus on the reasonableness of the volume of information sought, and the likely burden that would create for the bank. Justifications for requests, as part of the internal authorisation process, were frequently inadequate. The NZSIS's governing operational policy also did not provide guidance about *how* to carry out a proportionality assessment.

19. I found that Service staff were reluctant to obtain customer information from banks pursuant to a warrant, with a strong preference for the voluntary disclosure process even when there was already an intelligence warrant in place for the particular customer. I accept this practice was motivated by a genuine concern not to unduly raise the bank's level of interest or concern about an individual customer by using a less formal process, but I do not think that is an adequate justification.

20. Our case analysis sample was intentionally limited to cases from a three month period in 2016. From the collated requests we selected 13 cases for examination in greater detail. They disclosed issues that are relevant to the NZSIS's compliance requirements in this area.

21. Investigators sought to obtain extensive information under the voluntary process. Generally it was in the order of a few months of bank account and transaction history, but in some cases it was up to 12 or even 24 months' worth of data. The requests that were ultimately put to the bank were not always this broad after internal scrutiny and authorisation processes, however, some were. The Service's document management system was not organised in such a way that I could independently and readily check the subsequent records received.

22. Given the nature of the information sought and obtained in some of the cases examined, I found that very intrusive requests were at times made when the Service should have endeavoured to obtain an intelligence warrant to require the banks to provide the information. In my assessment many of the letters sent to banks should have also been clearer on their face that the requests were for "voluntary" disclosure.

23. I found that there was generally insufficient information in the requests to banks, particularly in terms of providing the bank with the necessary objective basis to justify the disclosure. The Supreme Court decision in *Alsford* confirms that requests should provide "some indication" of

why the information is needed, as this allows the external agency to assess the legitimacy of the request for itself. The response might be made that the Service is a covert intelligence agency, dealing with sensitive secret operations, and disclosure of any indication why the information is sought is not an option. That may be so in some, even many, cases. But in those cases the strict and express statutory secrecy attaching to intelligence warrants is a factor that the Service can weigh when considering whether an intelligence warrant, authorising it to require the production of information by the bank, is the more appropriate option.

24. It was not clear to me during the review whether the Service considered it had any special responsibilities towards banks or their customers when making requests for voluntary disclosure. The Service has subsequently confirmed it has a duty to provide the bank with sufficient information to assist it to determine whether and to what extent the bank can properly respond to the NZSIS's request.

25. Interviews with Service staff indicated that the financial information received from banks is retained indefinitely. It is stored in electronic document systems, which protect privacy and security by placing electronic limits on the information that particular staff can access. There are automated logs recording user activity these are subject to random internal audit. Beyond these measures, however, there was a lack of process to treat the information obtained from the banks in a way that ensured "minimal intrusion" — by which I mean, no regular systematic audits of access, and no ongoing reviews for relevance of the information. There was no organisational expectation that personal information obtained by this mechanism which was not, or no longer, relevant to an investigation would be destroyed.

Conclusions from Review

26. Service policies and procedures provided some effective guidance for NZSIS staff and enabled a degree of record-keeping, but did not adequately ensure compliance with all relevant legal obligations. I did not make formal individual assessments of the legality or propriety of particular case requests, but, based on my review of the sample of cases, although over a short period, it is likely that some of the past collection constituted unreasonable searches contrary to s 21 BORA.

27. Where the Service sought more than minimal personal information from the banks there should have been guidance directing staff to consider obtaining an intelligence warrant, or to seek the information under an existing warrant if there was one. Guidance should have advised Service staff on the circumstances necessary for an information request to be lawful and, in all the circumstances, reasonable. Guidance should have reflected that *from the perspective of the individual customer* the rigour of the warrant process is an important protection for personal privacy interests.[13]

[13] I discuss below the Ministerial Policy Statement (MPS) entitled *Requesting information from agencies under section 121 of the Intelligence and Security Act 2017*. Paragraph 29 of that MPS reinforces this principle.

28. I consider that the Service's policies should have stipulated that when making requests for voluntary disclosure Service staff should take specific account of the bank's duty of confidence to its customers. The likelihood that personal banking information will be subject to an obligation of confidence should be one factor considered in every case when the NZSIS is trying to determine the extent of a person's privacy interest in the information to be sought from a bank.[14] I note also that the new Act expressly recognises that the voluntary disclosure of personal information by an agency under s 122 of the ISA is subject to "any obligation of confidence".[15] It seems to me that it is for the Service, as well as the banks, to reflect this factor and give it appropriate weight in the way they approach their respective legal responsibilities and in the way they design their respective policies governing voluntary disclosures. The Service has indicated it will engage with the banks about its approach to voluntary disclosure in order to inform the banks' consideration of future requests.

Relevant changes under the ISA

29. The changes instituted by the ISA resolve some of the issues identified in the previous section. There are now three options under the Act for obtaining personal banking information: mandatory disclosure pursuant to warrant, mandatory disclosure pursuant to a business records direction,[16] or a request for voluntary disclosure of information to any person in the public or private sector under s 121.[17] The MPS includes a direction that requests for the voluntary disclosure of information under s 121 "must be identifiable as a non-enforceable request, rather than a demand with which the recipient is legally required to comply."[18]

Mandatory disclosure

30. Under the ISA there are now two mechanisms which the Service can use to compulsorily obtain information from other agencies: intelligence warrants or pursuant to "Business Records Directions."

31. The new business records regime addresses the New Zealand Bankers' Association concerns about voluntary disclosure of customer information.

32. "Business records" relate to certain information, defined in ISA, and held by telecommunications network operators and financial service providers.[19] The Service may apply for a Business Records Approval, a standing authorisation for particular categories of records. An application by the Service for an Approval to obtain business records must address necessity, proportionality and privacy impacts. It also has to explain why it would be

---

14 *Alsford* at [68] and [71].
15 ISA, s 122(4)(c).
16 ISA, part 5, subpart 4.
17 ISA, part 5, subpart 1.
18 Ministerial Policy Statement (MPS) *Requesting information from agencies under section 121 of the Intelligence and Security Act 2017*, ("s 121 MPS") at paragraph 21 under the heading "*Legality*". I explain the role of MPSs at paragraph 38, below.
19 ISA, s 144.

"impractical" or not be "more appropriate" to apply for a warrant authorising the seizing of business records. Approvals are issued by the responsible Minister and the Chief Commissioner of Intelligence Warrants who can impose any restrictions or conditions. My office reviews all Business Records Approvals issued under the Act, as we do warrants.

33. If a relevant Business Records Approval is in place a Director-General may issue a Business Records Direction to a business agency, seeking particular records. As part of this process, the Director-General too must consider the necessity for and the proportionality of the direction.[20] The banks (along with other financial service providers[21]) are now compelled when issued with a business records direction to provide the information specified.

34. The benefit for the banks is that once a business records direction is issued, they are required by legislation to comply and, both for the banks and for the Service, there is a clear legal basis for the disclosure under the Business Records Approval, without the need to obtain a warrant in every case.

35. ISA requires the Director-General of an intelligence and security agency to keep a register of all business records directions issued by him or her.[22] Undoubtedly this regime has the potential to be a far more exacting process for the NZSIS.

36. I informed the Service of my opinion that the first set of Business Records Approvals (which are, in substance, standing authorisations to "search") were too broadly drafted and provided inadequate criteria and parameters to guide and constrain the issue of subsequent directions (ie the actual requests).[23] In my view very broad Approvals raise problems of legality, akin to those posed by "general warrants". The Service undertook to consider my concerns, and it has done so. The latest iterations of Business Records Approvals, issued in September 2018, satisfy most of my concerns. There is scope and opportunity for further changes and improvement as practice develops, given that Approvals expire every six months. I will monitor any changes, and prepare a brief report when I have completed my foreshadowed review of the Service's approach to the business records regime.

Voluntary disclosure

37. The new Act also has a framework for voluntary requests (ss 121 and 122). These provisions do not create a new stand-alone legal basis for the disclosure of information to the intelligence and security agencies. Rather, they recognise that disclosure under the existing law may lawfully occur where there is no legal impediment. The purpose of the provisions was

---

20 ISA, s 150(3).

21 A "financial service provider" is defined by s 4 of the Financial Service Providers (Registration and Dispute Resolution) Act 2008.

22 ISA, s 153.

23 The same concern arises for requests to telecommunications network operators, who are also subject to the Business Records regime in subpart 4 of part 5 ISA.

to make the agencies' access to information more transparent and to make it clear on the face of the agencies' own legislation that these requests and disclosures occur.[24]

38. The Minister responsible for the intelligence agencies has issued a Ministerial Policy Statement (MPS) specifically on how the agencies should approach voluntary requests under s 121.[25] MPSs are a new instrument under ISA intended to ensure that the agencies act properly in the conduct of their lawful activities. The MPSs provide authoritative guidance to the NZSIS and the GCSB who must have regard to them. MPSs should be used to resolve statutory uncertainty, and to answer the question of whether the agencies "should" do something as opposed to whether they "can". The principles in this particular MPS reflect most of the principles I have identified in this report.

39. In the banking context, I consider there is no scope for a personal information request process that entails anything more informal, or more ad hoc, than the procedure provided in s 121.

40. In addition, given the real risk that almost all requests for personal information from a bank will constitute a "search" I see limited scope even for requests under s 121. The business records regime, rather than s 121, should be the default mechanism, assuming it is not impractical or not more appropriate in the circumstances to obtain a warrant.

41. For the banks' part they are required,[26] before disclosing information in response to s 121 requests, to consider their obligation of confidence in relation to information requested. Where NZSIS makes a s 121 request it will need to provide sufficient information on which a bank can make an assessment about the lawfulness of its disclosure. A certificate can be provided by the Director-General to support the request.[27]

42. The Service has responded to a draft of this review report, making the point that it is very conscious of the role of s 21 BORA in this context. I welcome the Service's assurance to me that: "voluntary disclosure can and will only be requested in respect of information in which the customer does not have a reasonable expectation of privacy and, as such, any such request will not amount to a search. Where voluntary disclosure is requested for information in which a customer would have an expectation of privacy (for example, in situations of urgency), this will only occur where doing so would not constitute an unreasonable search." The new Service policies I have seen confirm that assurance, and I expect to see it reflected in the overarching framework to be developed pursuant to recommendation 2 of this report.

---

[24] Departmental Report to the Foreign Affairs, Defence and Trade Committee, on the New Zealand Intelligence and Security Bill, paras 721 and 744.

[25] Issued pursuant to s 206(g) ISA, the "Section 121 MPS". Relevant also is the further Ministerial Policy Statement which covers informal and/or covert "collection" of information: Ministerial Policy Statement, *Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78 of the Intelligence and Security Act 2017*.

[26] ISA, s 122(4)(c).

[27] Certificates are issued by the Director-General certifying that he or she believes on reasonable grounds that the disclosure of the information is necessary for the performance of any of the agency's functions, s 122 ISA.

43. Retention of irrelevant information has emerged as an issue since the ISA came into force. The Act is clear that if material obtained under a warrant or Business Records Direction is assessed to be irrelevant to any specific function of the agencies under the Act it must be destroyed.[28] However, the Act does not have a similar provision that deals with information obtained by means of activities that do not require specific authorisation, such as voluntary disclosure.

44. I have advised the Service that in my view it should have internal policies to ensure that financial business records obtained by voluntary request under s 121 are stored appropriately and regularly assessed for relevance. Personal information, obtained covertly through Service requests, and known to be irrelevant or later found to be irrelevant, should be deleted. If a disposal authority from the Chief Archivist under the Public Records Act 2005 is required in order to do that, I believe one should promptly be obtained. I do not think that indefinite retention is sound as a matter of law or propriety. I see no justification for personal information, obtained under a voluntary disclosure process, to be treated so differently to information obtained by mandatory processes.

A coherent framework is needed

45. A priority for the Service now is to develop a coherent and workable framework for how the three mechanisms under ISA for obtaining personal information from third party agencies operate and interrelate.[29] In particular, the framework should clarify when a warrant is a more appropriate mechanism than a business records direction. It must reflect the significance of s 21 BORA and the definition of "search" as confirmed in *Alsford*. In addition, however NZSIS draws the line between use of warrants and Business Records Directions, the framework should expressly recognise that the business records regime was not intended to allow access to "bulk" or "class-based" requests for information.[30] In my view Parliament envisaged that if large volumes of personal information, or non-specific information, is needed that should be obtained under a warrant.

46. Specifically with respect to obtaining banking records, the framework should confirm the limited scope for voluntary disclosure and ensure due recognition of banking customers' privacy interests.

---

[28] ISA, ss 103 and 152.

[29] Warrant, Business Records Direction, and Voluntary request under s 121.

[30] New Zealand Intelligence and Security Bill, Commentary as reported from the Select Committee, at 8. See also the discussion in the Committee of the House, 16 March 2017, where the then Minister responsible for the NZSIS and GCSB, the Hon Christopher Finlayson, said: "…the ability to go for a general trawl is simply not there. These are very carefully crafted procedures, which are set out, and it is not going to allow for large scale or bulk access to information. Every request is going to need to be made with reference to a specific person and so on."

RECOMMENDATIONS

47. Recommendation 1: Having consulted with the Privacy Commissioner on this report, I recommend that the NZSIS should keep a record of all requests for customer information made to financial institutions, under any mechanism, including those made under s 121 ISA. This record will facilitate the monitoring of the type and frequency of requests for disclosure of information from banks, and will support my oversight function.

48. Recommendation 2: The Service should prioritise the development of a clear and comprehensive framework setting out when s 121 ISA, a warrant, or a Business Records Direction should be used. The framework must ensure that resort to each mechanism reflects the legal considerations addressed in this report and in the relevant MPSs.

49. Recommendation 3: I recommend that the Service reconsider its position on the retention of "irrelevant" information obtained through the voluntary request process. The Service should examine this issue through a broader policy lens and obtain advice from the Privacy Commissioner and the Chief Archivist and, if there remains any doubt, from Crown Law.[31]

[31] By the time I prepared this public version of the report the Service had acted on this recommendation and sought the advice from the Chief Archivist and the Privacy Commissioner. The process is being worked through. It may well be that a disposal authority from the Chief Archivist is needed in order to dispose of irrelevant personal information obtained by voluntary requests.