Office of the Inspector-General of Intelligence and Security

Lawfulness of NZSIS access to data under the Customs and Excise Act 1996 and the Immigration Act 2009

Cheryl Gwyn
Inspector-General of Intelligence and Security

14 December 2017

Contents

INTRODUCTION

1. This review[1] concerns the lawfulness of NZSIS access to Customs and Excise Act 1996 (CEA) and Immigration Act 2009 (IA) data. I commenced it in late 2014/early 2015, and have reported on its progress in three of my Annual Reports (2014/15; 2015/16; and 2016/17).

2. The information collected and held by the Customs service ("Customs"), under the CEA, concerns persons, goods and craft crossing the border. NZSIS has used that information for two specific functions: intelligence searches and "travel alerts". Information for both of these purposes could be obtained by certain NZSIS officers who had access to the relevant Customs' database, referred to in this report as CusMod. The Immigration New Zealand ("INZ") information is airline passenger check-in information, known as Advance Passenger Processing information, or APP. I discuss both sets of information and how they were accessed below.

3. The practice of NZSIS (or "the Service") accessing CusMod and APP data came to my attention in late 2014 as a result of two developments:

    3.1 In September 2014 the Director of the NZSIS notified me and the Privacy Commissioner of three NZSIS proposals to access, use and retain APP data collected under the IA. These proposals, in various ways, involved data matching of incoming passengers, including against their past travel movements. The proposals required NZSIS to receive INZ's APP data and then make its own copy to enable the cross-checking process.

    3.2 On 25 November 2014 the Countering Terrorist Fighters Legislation Bill was introduced. It was enacted under urgency two weeks later. It amended the CEA to provide in s 280M for access by the NZSIS to databases compiled under that Act. This amendment was made to address concerns about the basis upon which access up to that point had occurred. I was aware of that issue, and my office commenced discussions with the Service. Other questions then arose, because, as this report finds, access by NZSIS under the new access mechanism was not subsequently in accordance with it.

4. My review process has been drawn out, but I see no benefit in explaining that timeframe in detail here. It is sufficient to say that there has been a large volume of correspondence, of an iterative type, between my office and the NZSIS over the many separate legal issues that arise. The NZSIS has also obtained external legal advice at various points[2] and has conducted an independent review in relation to its CusMod access, which, among other things, resulted in identification by the Service of certain "lessons learned". All of this has taken time. Because of the communication process we have followed, including a substantive report that I provided to the NZSIS in May 2016, the NZSIS already has a clear picture of my concerns, reasoning and core

---

1 Pursuant to s 11(1)(d)(ii) of the Inspector-General of Intelligence and Security Act 1996 ("IGIS Act").

2 Legal privilege in any advice relating to these matters is not waived by the Service, and I have expressly had access to, and considered, that legal advice in the course of this review on the basis that privilege is not waived.

findings. The purpose of this report is to publicly set the matter out in so far as I can, and state my findings and recommendations in final form.

5. The scope of my role, which is to oversee all aspects of the NZSIS's conduct, means that I am as interested in the systemic matters and the broad issues of agency approach to law and compliance that arise, as I am in how the agency responds to (and remedies) any particular legal problem. Some of the comments I make in this report are squarely of that broader type.

ACCESS TO CUSMOD AND APP INFORMATION

6. Customs and INZ have specific functions relating to the movement of people and goods in and out of New Zealand. To give effect to these functions they have statutory powers to obtain, use, and store particular information. The extent of information-gathering under those two Acts is substantial, encompassing, I am told, approximately 11 million passenger movements each year including, over time, data relating to a large proportion of all New Zealanders. It is also material that, for New Zealand citizens in particular, only limited use is made of IA data even by INZ, as the only decision-making permitted under the IA is to ascertain whether New Zealand citizens have a valid passport. NZSIS, however, over the relevant period had access to information in these datasets for its own purposes, including on occasion providing specific intelligence on security grounds to agencies in other countries.

7. I recognise that there are genuine and internationally recognised reasons why domestic intelligence services might need access to Customs or INZ data. The issue for me as the Inspector-General is whether that access occurs in accordance with New Zealand law: what is the legal basis for particular access? Are there limitations on access, and subsequent use? If so, are they adhered to? What steps are taken to remedy any unlawful access, retention or use?

CusMod data access

8. NZSIS has had access to a limited volume of information held on the Customs Modernisation Scheme Database (CusMod) through a dedicated Customs computer terminal, physically housed in NZSIS premises, since CusMod was set up in 1997. CusMod contains information about border crossings by people, goods and craft and is an essential source of intelligence collection for NZSIS. NZSIS has used (and still uses) CusMod in two discrete ways: "travel alerts" and "intelligence searches".

Travel Alerts

9. NZSIS can load travel alerts against persons of pre-identified security or intelligence interest to monitor their border crossing movements. To do this, NZSIS accesses the dedicated Customs computer terminal and enters the known identifiers of the person into the travel alert function (e.g. name, passport number). If that person later crosses the New Zealand border the travel alert will "hit" and the details of that hit will be automatically delivered to a "work queue" which is located in CusMod in the NZSIS interface.

Intelligence searches

10. The second primary function is "intelligence searches." Up until November 2014, when technical access was suspended (see below), NZSIS officers could log on to the dedicated Customs terminal, using the NZSIS logon and purpose-built NZSIS interface, to conduct a search of CusMod for intelligence relating to a pre-identified entity of security or intelligence interest, or for the purposes of conducting a security clearance assessment.

APP data access

11. APP is mandatory information collected at check-in for all incoming (and most outgoing) international airline passengers and crew (including all transit passengers). It was implemented by INZ in August 2003 as part of the Advance Passenger Screening (APS) system, designed to assist in the identification and screening of passengers prior to boarding an aircraft. The system enables airlines to check – before the passenger boards – the validity of their passport and visa, as well as for checks to be run against INZ border agency alerts. It enables an offshore border security component. APP sharing of this dataset with NZSIS has happened since 2011.

12. APP contains significantly less information than is available to check-in staff or Customs officials. It does not include photographs, addresses, booking details, credit card numbers, seat numbers, dietary requirements, frequent flier numbers, or details of any onward travel. Information contained within each APP entry falls into two general categories :

    12.1 Information identifying the individual traveller, such as name; passport or certificate of identity number, and expiry date; date of birth; nationality and gender.

    12.2 Information identifying the craft and its intended movements, eg. airport check-in and flight codes, and expected arrival date/time.

13. APP sharing allows near real time data matching. In simple terms the mechanics are that NZSIS requests INZ to provide all check-in events. INZ generates these and sends them electronically, at regular short intervals, to NZSIS, whereupon they are transferred to NZSIS's internal computer systems for automatic matching.

FINDINGS IN RESPECT OF LEGALITY OF CUSMOD ACCESS

14. As described above, long-standing practice was that NZSIS had access to a dedicated CusMod terminal to carry out intelligence searches and to set and retrieve travel alerts. On 24 November 2014 all NZSIS access to the dedicated CusMod terminal was temporarily suspended in relation to both intelligence searches and travel alerts. This was the result of concerns identified by various Government agencies involved as to the legal basis upon which NZSIS access occurred.

15. On 12 December 2014 s 280M CEA came into force to provide a legal authority for NZSIS direct access to CusMod data.[3] It explicitly authorised NZSIS (and NZ Police) to directly access CusMod to search the database, but only for counter-terrorism investigation purposes. Section 280M required any direct access by NZSIS to CusMod information to occur in accordance with a written Memorandum of Understanding ("MOU") between the Director of Security and the Chief Executive of Customs.

16. From 19 December 2014 to 19 December 2015 an Interim Arrangement, of a type permitted by the combination of ss 6[4] and 280M CEA, was in place to allow access. There were limitations, however, on NZSIS access to CusMod, compared to the situation prior:

    16.1 The Interim Arrangement was limited to NZSIS "creating, amending and verifying travel alerts." It did not extend to "retrieving" travel alert hits.

    16.2 The Interim Arrangement provided that NZSIS access would be limited to five specified NZSIS officers, who would be provided with individual log-on credentials.

    16.3 Section 280M permitted access only for counter-terrorism investigations.

17. NZSIS subsequently identified (and I concur) that it breached each of these constraints over the relevant period:

    17.1 Travel alert information was retrieved directly by NZSIS (ie. hits about particular individuals' travel movements).

    17.2 The logons for the five officers were not set up and used, and no technological block was put in place to limit access by NZSIS staff. As a result, NZSIS staff other than the five approved officers accessed CusMod.

    17.3 The CusMod travel alert function was used to retrieve data for purposes other than counter-terrorism investigations.

18. Somewhat overlapping with this, on 18 August 2015 the permanent MOU, under s 280M, was signed and came into effect. This too required NZSIS to identify specific staff who could have access to CusMod. NZSIS requested this status and associated logon credentials for 17 staff. The logons were not received, however, and, despite this, other staff continued to access CusMod. There was no evidence of any follow-up by NZSIS in relation to the person-specific logons. This

---

[3] It was always legitimate for NZSIS to make case-by-case requests to Customs for information relating to a specific matter or person, or for a particular purpose, and they would be assessed on their merits. By contrast, s 280M concerned NZSIS's own remote access to bulk CusMod data.

[4] Section 6 CEA permits the Chief Executive of Customs to "authorise" in writing certain people who are not Customs officers to exercise any power or function under the CEA.

situation lasted until 15 June 2016 when all NZSIS staff were directed to cease accessing travel alert information on CusMod.

19. In summary, I find that, for the reasons set out below in this report:

19.1 Prior to 24 November 2014 NZSIS acted unlawfully in obtaining information from CusMod by conducting intelligence searches, and by its use of the travel alert process.

19.2 From 24 November 2014 until mid June 2016 NZSIS continued to illegally access CusMod for travel alert information[5] via processes that were not consistent with the authorising regime. That access was unlawful in itself, and on the occasions the access was not for counter-terrorism purposes the purpose of access was also unlawful.

20. As a result of legal advice, in June 2016 the NZSIS's Compliance team investigated the shortfalls in access procedure, and addressed them. I am satisfied that from August 2016, when NZSIS access to CusMod resumed, it was lawful. From August 2016 to 30 March 2017 access was in accordance with s 280M CEA and the MOU. This permitted both intelligence searches and travel alert information to be accessed for counter-terrorism investigation purposes only. Since 1 April 2017 access has occurred pursuant to a Direct Access Agreement, made in accordance with s 125 of the Intelligence and Security Act 2017.
www.nzsis.govt.nz/assets/media/Direct_Access_Agreement_Customs.pdf

21. I do not know the likely total volume of data in question, nor have I seen policies governing how this unlawfully obtained data is to be managed from this point. In May 2016 I provided NZSIS with a report on my findings to that date. It included the finding that the CusMod travel alert access was unlawful. One of my specific recommendations was that NZSIS investigate and report upon the extent to which it has accessed CusMod data. I have not received a comprehensive analysis which shows the scope of the data received unlawfully by NZSIS from CusMod since November 2014, let alone prior. Nor has NZSIS acted on my recommendation to discuss remedial steps with me and the Privacy Commissioner. I understand that this is because the Service does not consider its "travel alert" access to have been unlawful. Nor have I received a report on the extent of the historic "intelligence search" access either.

22. The NZSIS has improved its compliance processes,[6] and also now has a dedicated compliance team. The changes to the CEA and the new Intelligence and Security Act 2017 now provide a lawful basis for both forms of CusMod access. However, I remain concerned by the Service's failures to:

---

5 Intelligence searches were not conducted between November 2014-August 2016.

6 My latest Annual Report (2016/17) records that I have found this year that the Service's compliance systems are sound, notwithstanding that particular compliance issues may arise. One positive development stemming in part from the CusMod "lessons learned" process has been the identification the Service of the importance of a dedicated compliance team.

22.1 Expedite the process of obtaining definitive legal advice on the particular issues once the basis for concerns was raised. (A positive step, which I have recognised in this report,[7] is that in the related context of APP data the potential problem with access to and use of that data was originally drawn to my attention proactively by the Director of the NZSIS.)

22.2 Achieve timely clarity on any specific legal matters over which it retains doubts, or if there is ambiguity. This point takes on considerable significance as the NZSIS has confirmed to me recently that it still does not accept its access to the travel alert information was unlawful. The Service's position is that the legal advice it received from the Solicitor-General may not have been focussed on that particular travel alert access process. I read the advice differently. In holding that interpretation I also bear in mind the volumes of correspondence around this matter over the last few years, and the legislative amendments. In any event, I do not consider that relying on doubt or ambiguity in legal advice is a responsible and risk-averse approach.

22.3 Directly respond, in a timely way, to my office's queries over time as to the specific basis for lawfulness, the extent of any unlawfully obtained material, and the steps for remedy. We have largely got there in the end, but on balance I have found the Service reluctant in its engagement with me on this matter. I have also been at times delayed and waylaid by NZSIS's lack of precision and forthrightness in responding to my office on specific issues.

22.4 Provide me with certain original and unredacted documents I requested. In particular, the Service declined to provide a copy of the original independent report it commissioned, and some of its internal legal advice. I am entitled to this material under s 20(1) of the IGIS Act 1996.[8] I appreciate that there are many sensitivities to be balanced in such situations, but I am capable in this role, and more than willing, to weigh those matters and treat them appropriately. The lack of these documents obstructed my ability at particular points in time to get the full picture of the Service's view of its operational conduct. Nonetheless, while it would have assisted my oversight role to have had these documents, it has not prejudiced my ability to inquire properly into this matter, and make firm findings.

FINDINGS IN RESPECT OF LEGALITY OF APP ACCESS

23. After much consideration, I am satisfied that the different wording in the CEA and IA permit different data sharing arrangements with NZSIS. Further, the way in which the APP information was obtained by NZSIS was materially different to the way in which the CusMod travel alert information was obtained. As a result, I accept that NZSIS did not have "direct access" to the APP information in the same way it did CusMod. The Service has obtained specific legal advice

---

7 See paragraph 3.1, above.

8 That right is now repeated in s 217 of the Intelligence and Security Act 2017.

on its access to APP information, and I am satisfied that this aspect of the review needs no further consideration by me.

24. There remains the issue of the use to which APP data obtained prior to the Direct Access Agreement, under s 125 of the Intelligence and Security Act 2017, can be put. The issue arises because the purposes for which APP data could be obtained under the prior legislative regime are less broad than under the new framework. The NZSIS has confirmed that, as a matter of practice, it has not to date used the information from the "stored" APP data. I make a recommendation in relation to this issue at the end of this report.

REASONING AS TO UNLAWFUL ACCESS OF CUSMOD

25. NZSIS accepts that it acted without lawful authority (and thus, unlawfully) in conducting intelligence searches on CusMod data prior to 24 November 2014. I have found there was no subsequent unlawful access after this date for the purpose of intelligence searches.

26. As I have stated above, the Service asserts, by contrast, that its access to travel alert information was at all times lawful. NZSIS has, over the course of this review, suggested various legal rationales for this, which the Service and I have then gone on to discuss and examine more closely. The Service's final position, confirmed in late 2017, is that its access to travel alert information prior to June 2016 was legal because it did not have "direct access" to CusMod.

27. In asserting a lawful foundation for obtaining CusMod travel alert data NZSIS has consistently relied on, and continues to rely on, a combination of a common law ability to ask for information from any agency and receive the recipient's answer ("ask and answer"), and s 57 of the Privacy Act 1993.

28. I summarise briefly below my own legal analysis of why NZSIS's access to the information in question was unlawful:

    28.1 At the relevant time there was no express statutory provision in the CEA to permit Customs to "disclose" the particular information to NZSIS, or to permit NZSIS to "access or obtain" Customs information. There were a number of express provisions in the CEA addressing information sharing with specific bodies, or the sharing of a specific type of information (including with NZSIS), but they did not apply to the information in question.

    28.2 The CEA contained a detailed information access scheme, permitting disclosure to a number of agencies for specific purposes. However, s 282A of the CEA (prior to s 280M) provided the only statutory provision upon which Customs could share or disclose to NZSIS (or NZSIS "access") personal information (ie. information about an identifiable individual) in CusMod.[9] In this statutory context there was no scope for routine "ask and

[9] In my view it probably also provided the sole basis upon which any "non-personal" information could be shared, but I do not need to make a finding on that.

answer" to operate alongside s 282A. The scheme and specificity of the CEA provisions tells strongly against "reading in" a power for NZSIS to access information not addressed by that scheme.

28.3 The information sharing in question did not occur under s 282A CEA.

28.4 Neither s 4(1)(a) of the NZSIS Act (the Service's own governing legislation at the time), nor any other provision in its Act, provided a power to access the information.

28.5 Section 57 of the Privacy Act (as it was prior to amendment in 2017) is not an empowering provision – it does not give a positive authority for NZSIS to obtain information from any agency, whether private or public. It does not, and cannot, reasonably be read to infer a power of access to data collected under other legislation that also contains specific provisions tightly regulating access to that data. The effect of s 57 was to provide an exemption from certain Privacy Act controls, not to provide a power of access.

28.6 "Ask and answer": for the reasons given above concerning the particular statutory framework Customs did not have a power to share the travel alert information in bulk. As a result, receipt or access – certainly on a large scale, systematic basis, at NZSIS's will – was unlawful by NZSIS. Further, there is no proper analogy between a common law power to ask another party to disclose records about a particular matter or individual (ie. a case-by-case request) and the extensive powers that the Service was purporting to use – a comprehensive data-matching power, or a power to access all of another party's records of a certain type. The ask and answer process, properly and responsibly conducted, would require the NZSIS to demonstrate to the other agency that it has proper reason to obtain specific information, so that the requested agency could make an informed decision in the particular case. That did not happen.

29. In my view, it goes without saying that it is important for the State to always approach "ask and answer" requests in a transparent and case-specific way where there is personal information at stake. Private individuals have legitimate expectations of privacy in, and proper use of, their information, including when the State is attempting to carry out legitimate public interest functions.

30. As I understand it, the Service largely accepts the above legal analysis, and accepts that there was no basis in law to directly access CusMod for travel alert information. It says, however, that on the specific technical facts, NZSIS was not "directly accessing" it; instead it was engaged in "an automated ask and answer process", and that was lawful. The Service has recently explained in short form the mechanism by which it received the information:

> "NZSIS sent a detailed request to Customs for information of any border crossing by a person matching the details NZSIS provided. Customs then automatically matched and generated the data when it arose, and then sent

advice to NZSIS that it could collect the information from the NZSIS interface."

31. For many reasons I do not think this approach, or this formulation of the mechanism for receiving the travel alert information, assists the Service. In brief, in response to the main contentions raised with me:

31.1 The critical point is the one I make above: Customs had no power to share in bulk the travel alert information with NZSIS; as a result, an unlawful sharing occurred when NZSIS received information from Custom's database. Ultimately the finding of unlawfulness rests on this point. I am compelled also to add that in the travel alert process NZSIS was not an unwitting or minor participant. This matter involved routine sharing in which NZSIS was an active and on-going party, if not the lead player.

31.2 The statement at paragraph 30 above downplays the Service's role. NZSIS staff physically accessed the CusMod terminal. They directly (ie, themselves) entered information in CusMod which set the requirements for a future data match. They again, themselves, retrieved information from CusMod when it triggered a hit. I have approached my analysis of this matter on the detailed written description provided to me in 2017 by the Service's own "lessons learned" report.[10] It is unconvincing to represent NZSIS as a "requester" but not a "retriever" or "accessor" of travel alerts in this process.

31.3 The analogy with a genuine ask and answer process is specious. The NZSIS was not making specifically justified requests, on a case by case basis, in response to which Customs was making a decision.

31.4 Steps taken since late 2014 to provide specific legal authority for NZSIS travel alert activity point strongly towards NZSIS having acted unlawfully by "directly accessing" CusMod prior to that. In this regard, I note the enactment of s 280M, and the new "direct access" regime authorised by s 125 of the Intelligence and Security Act 2017.[11] I appreciate, of course, that enactment of a permissive power does not in itself establish that prior conduct without that empowering provision was unlawful, but it is a reasonable view in the present case that the legislation was necessary to avoid on-going illegality. I further note that NZSIS's own current policy on access to Customs databases uses the terminology of "…may access any NZCS database directly…. to add or amend alerts." The short point is that none of these instruments – the Acts, MOU, Direct Access Agreement and internal policy – depict NZSIS as receiving information disclosures from Customs as part of a request process when carrying out the travel alert function; rather, the Service

[10] I have summarised the material addressing the CusMod access process at paragraphs 8-10, above.

[11] Both statutory provisions have headings which use the words "Direct Access". Section 280M speaks of "access by" NZSIS "to information stored in a database", and the Chief Executive of Customs may "allow" certain NZSIS officials to "access the database". "Access" is defined to "include remote access." This language reflects the reality of how the information sharing was occurring at that time: NZSIS itself "accessing" the database.

is depicted as an external party with the capability to reach in and access the Customs' information infrastructure in question. In my view that is an accurate statement of what has occurred here, and in common terminology that is "direct access".

32. This was systemic unlawful access on a large scale. The access since late 2014 is more troubling again, as the Service was, from that point, expressly on notice that access – unless properly empowered and regulated – was unlawful; or putting it at its best from the Service's perspective, very likely to be unlawful. The NZSIS' failures over the best part of two years to adhere to the terms of the Interim Agreement and the MOU are significant and hard to fathom.

33. While I have found the Service's access to CusMod data over the relevant time was unlawful, I recognise that the Service did not wilfully breach the law. It also seems to me that only in the last few years has focused consideration been given at sufficiently high levels in Government to the legal mechanisms that permit access by one Government agency to information held by another Government agency.

34. My preference in respect of illegally obtained data that has been retained or shared is that the Service identifies it, and deletes the material it can.[12] If deletion is not technically possible, it should remove access to that data and find a mechanism to ensure that retained data is "tagged". This will help ensure that future use is limited or avoided.

RECOMMENDATIONS

35. In light of these conclusions, I make three recommendations to address the consequences of the unlawfulness of NZSIS access to CusMod intelligence search data (prior to 24 November 2014) and to travel alert data (up until mid June 2016), and to address my outstanding uncertainty and concern around how the NZSIS might treat the stored APP data:

    35.1 The NZSIS investigate and report to me on the extent to which it has illegally accessed CusMod data.

    35.2 The NZSIS discuss and agree remedial steps with me and with the Privacy Commissioner in relation to that data. My preferred approach is set out above, at paragraph 34.

    35.3 The NZSIS satisfies me that there is a clear basis to retain the APP data obtained prior to 1 April 2017[13] for the purposes of using it as if it had been obtained under the 2017 Act. If and until that has been done the data should not be used in any way by NZSIS.

---

[12] This approach is consistent with that taken in s 203 of the Intelligence and Security Act 2017 to unauthorised information obtained by the intelligence agencies.

[13] The date on which s 125 of the Intelligence and Security Act 2017 came into force, permitting direct access for all of the purposes specified in the Direct Access Agreement www.nzsis.govt.nz/assets/media/Direct_Access_Agreement_Customs.pdf

36. Given the delays in completing this review, I put a timeframe on receiving substantive responses to my recommendations within three months from the date on which I provide the Service with a copy of this report.