Office of the Privacy Commissioner submission on the Customs and Excise Act Review Discussion Paper

8 May 2015

Privacy Commissioner
Te Mana Matapono Matatapu

Introduction

The Customs and Excise Act 1996 (the Act) governs the New Zealand Customs Service's (Customs) work at the border. Since the Act was developed, Customs' operating environment has changed significantly. The legislation needs to be fit to operate now and into the future.

The issues identified in the discussion document can be addressed while still ensuring sound privacy-aware decisions are made.

We commend Customs for releasing a discussion paper to canvas the issues of modern border management and intelligence, and to prompt discussion while it explores new options. We hope that the feedback Customs receives on the document helps to define the problems Customs faces and find appropriate mitigations and new opportunities.

The Office of the Privacy Commissioner's (OPC) role covers a range of areas discussed in the document. Foremost among these are the approach to information sharing (both within government and with the private sector and agencies overseas) and use of personal information including, for example, biometrics and passenger name record (PNR) data.

We have some concerns regarding the approach the discussion paper takes to information sharing. The discussion paper suggests developing a bespoke, 'one-stop shop' approach for Customs that would cover all information sharing, whether personal information or business related. This is one possible solution, but also has risks. As Customs' analysis of solutions progresses, we expect to see other options for facilitating information sharing, as well as bespoke legislation, evaluated.

Concerning facilitating the sharing of personal information, options could include, for example:

- legislation – this could take the form of
    - specific provisions in the Act that provide more tailored protection to New Zealanders' personal information, or it could involve
    - an amendment to the Privacy Act's Schedule 5 – stating which information can be accessed and by who
- working with the Privacy Act's Information Privacy Principles as they stand, but providing clearer guidance to Customs staff about their abilities to use or share personal information
- an Approved Information Sharing Agreement
- a code under the Privacy Act providing greater clarity of information handling obligations
- amendments to governing statutes of other agencies Customs works with or other legislation which governs aspects of Customs' work with other agencies.

Given that the document serves to raise issues and prompt general discussion of Customs' future, we are not able to provide more detailed comment at this point in time.

We are working with Customs as it investigates options for reform, and we look forward to continuing engagement to ensure that New Zealanders' privacy is carefully considered and protected.

This submission covers a number of issues discussed in the discussion document. For ease of navigation these are organised under the original headings from that document.

Information

Customs' Information Framework and Goals

The discussion paper proposes the development of a coherent, transparent framework for collecting, using, storing, sharing and disposing of information. It asserts that the current framework is neither transparent nor coherent, and causes inconsistent approaches to information handling.

Given the Act's many changes, this is unsurprising. Since 1996 Customs' functions have broadened, and the degree of overlap and cooperation with other agencies required has increased. This has led to the development of ad hoc solutions.

As a standalone piece of legislation, the Act therefore currently lacks many of the privacy safeguards and provisions in terms of information sharing that would have been included if Customs' current role was anticipated in 1996. If a new framework was developed, existing privacy rights would need to be adequately safeguarded.

The process that Customs is undertaking provides an ideal opportunity take a 'first principles' approach. Before any new legislative regime is developed Customs will need to identify the short-comings of existing mechanisms to meet its requirements for current and future operations.

The analysis of options for legislative amendment should include a thorough review of the ability (and appropriateness) of the full range of existing mechanisms to enable Customs to achieve what it needs to.

ISSUE A: SHARING INFORMATION WITH SECURITY AND LAW ENFORCEMENT AGENCIES

The paper states that the existing legislative framework does not support new ways of working with domestic security and law enforcement agencies (e.g. The Police, The New Zealand Security and Intelligence Service, and the Ministry for Primary Industries) for purposes other than border protection.

As Customs notes in the document, direct access carries the risk of inappropriate access or sharing. Further analysis is required to determine whether direct access is the best mechanism.

A number of tools already exist to accommodate new ways of working with non-border agencies and facilitate sharing of personal information between agencies. For example, the Privacy Act provides for Approved Information Sharing Agreements (AISAs) which allow agencies to collaborate and share information, without intruding on individuals' rights or exposing agencies to legal risk (we have included some information on the applicability of an AISA at the end of this section).

In working with agencies to help them share information responsibly, our first point is to urge a very clear statement of the purposes for which that agency proposes to collect, use and share personal information. Access by other agencies may be permitted if consistent with those purposes, or by expressly permitted exception. Access to Customs data needs to have a clearly identified purpose. Any access to information should be in line with that purpose.

The paper also notes that consultation with the Privacy Commissioner, the Ombudsman and other affected parties would be necessary. We agree, and would expect Customs' purpose for sharing the information to be clearly defined as part of this process.

ISSUE B: SHARING INFORMATION WITH GOVERNMENT AGENCIES FOR BROADER GOVERNMENT PURPOSES

The paper proposes that, in order to allow information sharing for broader government purposes, the Act could include a wider range of purposes for which information can be shared. These could include regulatory compliance with other frameworks (e.g. energy conservation), trade promotion, service delivery by other agencies, or sharing revenue information with Inland Revenue.

The arguments presented in the paper do not on their own present a satisfactory case for changing personal information sharing provisions. If Customs finds that they do need improving, we strongly recommend that should be via the Privacy Act review and applicable across the government, not just for Customs.

Under the current framework, personal information can be shared where there is a valid reason to do so. For example, by applying the exceptions to the information privacy principles, using an AISA, or by utilising Customs' own regulation-making provisions.

ISSUE C: SHARING INFORMATION WITH OVERSEAS AGENCIES

Customs seeks clarification of its overseas information sharing powers, particularly on the types of information it can share and with whom. The paper suggests new opportunities would be available if Customs had more clarity in its governing legislation.

It proposes establishing a set of criteria in the Act to help determine whether information sharing is appropriate or not. These criteria will be easier to establish once Customs has clearly defined its role domestically and internationally, and from that a firm list of possible information sharing arrangements.

Once Customs has a clear view of the potential information sharing opportunities, and the personal information that may be involved, we will be able to provide more specific comment.

ISSUE D: SHARING INFORMATION OUTSIDE GOVERNMENT, AND ISSUE E: PROTECTING COMMERCIALLY SENSITIVE INFORMATION

The paper proposes explicit processes for sharing commercial information outside government and for sharing commercially sensitive information in general.

Sharing commercial information requires a very careful and considered approach, just as for the sharing of personal information. Maintaining public trust and confidence that Customs will keep both commercially sensitive and personal information secure is very important.

In a general sense, personal information associated with business activities is often considered to have a low privacy value. Businesses want potential customers to know they are in business, and how to get in touch with them. Risks can arise, however, where the personal and business affairs of sole traders are closely interconnected. It can be difficult to draw a line between where business activity stops and personal activity starts.

To mitigate these risks, Customs may wish to look to the work the Ministry of Business, Innovation and Employment (MBIE) undertook on the New Zealand Business Number (Bill

currently before the house). The new mechanism may facilitate solutions to some of these issues.

Approved Information Sharing Agreements

Before exploring new mechanisms for sharing information, the suitability of AISAs should be carefully examined. The AISA provisions were created as a response to perceived barriers to government information sharing, and provide more flexibility than the information matching provisions of the Privacy Act.

Both personal information and 'non-personal information' can be addressed within the Approved Information Sharing Agreement (AISA) provisions of the Privacy Act. While an AISA may facilitate sharing of 'non-personal information', it does not authorise it if there are existing statutory provisions restricting disclosure or use of that information.

AISAs may be particularly useful for initiatives where the benefits derived would not necessarily or primarily be to Customs, or they would extend to a number of agencies (e.g. trade-related issues affecting independent operators such as sole traders or transfer and sharing of biometrics or information to assist anti-crime initiatives). AISAs may also provide a framework to ensure personal information is appropriately protected where other mechanisms are used (e.g. MoUs, Regulations under the Act, or service-level agreements with industry).

Section 96C of the Privacy Act explicitly addresses the issue of personal and 'non-personal information' as follows:

> ***information sharing agreement*** *or* ***agreement*** *means an agreement between or within agencies that enables the sharing of personal information (whether or not the sharing also includes information that is not personal information) to facilitate the provision of a public service.*

Furthermore, section 96A defines the primary statutory purpose of the AISA provisions as

> *to enable the sharing of personal information to facilitate the provision of public services.*

Reviewing the protections for travel records

Passenger name record (PNR) data is unverified information passengers provide to commercial carriers for their reservation and departure/arrival control systems. The paper proposes removing the 28-day window for warrantless access to PNR data.

We strongly recommend that it be retained.

The current rules in the C&E Act do not require Customs to destroy PNR data at any point, and Customs does not currently do so. The possible adverse effects of this to date have been significantly reduced by the restriction imposed by the 28 day window.

Recent changes to the way Customs receives PNR data have increased the efficiency of this practice. Changes in the mode of delivery to Customs, that is by "push" from airlines rather than active collection by Customs, does not alter the need for restrictions once the PNR data is in Custom's custody.

Access to PNR data is carefully restricted by sections 38G-38K of the Act. Under these criteria Customs may only view PNR data without warrant:

- within 28 days of the travel (section 38H)
- where an individual has undertaken travel within the 28 day period (section 38I)
- in emergencies where a warrant would otherwise be granted (section 38K).

Furthermore, section 282A of the Act makes clear that Customs may only disclose information to other agencies for other purposes where it meets the criteria set out in 38G to 38K of the Act, including where it has been viewed under warrant (as provided for under section 38J).

Recent provisions in the Immigration Act 2009 concerning New Zealand Immigration's use of PNR data do not specify a retention period. Immigration's retention of the PNR data is dependant on the rules set out in the Act because Customs holds the data. Any review of PNR data protections should factor in interdependencies with other Acts.

NEW ZEALAND PNR PRACTICE IN AN INTERNATIONAL CONTEXT

PNR data covers all travelling individuals, whether or not they raise law enforcement, immigration or security concerns. Its collection and use has been the subject of significant debate internationally, and it is covered by International Air Transport Association guidelines which emphasise the need to preserve passenger privacy.

Over recent years, considerable work has progressed internationally, both at a regional level and through bilateral arrangements, to harmonise use of PNR Data and 'intelligence' information, both to facilitate global travel and trade and to support the prevention, detection, investigation and prosecution of serious crime.

Any proposal to change the way PNR data and related intelligence information is managed under the Act should take into account developing international norms in this area, including the need for proportionality in any use and disclosure of passenger-related information by law enforcement agencies, to ensure New Zealand's regime remains consistent with internationally-recognised best practice.

Technology and Digital Goods

Biometric Information

The paper proposes granting Customs new powers for the collection and use of biometrics. Outside of the operation of SmartGate, Customs currently only collects biometrics on behalf of other agencies, such as when acting as designated immigration officers.

Clarity in purpose for collection as well as appropriate limitations on use and disclosure under those purposes will be crucial if Customs chooses to develop provisions authorising collection and use of biometric information.

Biometrics allow the physical observation of a person's behaviour to be automatically linked with their identity and other information about them. With the development of biometrics that can be read from a distance such as facial recognition, iris scans, and the ability to identify individuals within a crowd, it is becoming possible to make this connection in real time, and without the individual being aware that they have been identified.

The Article 29 Working Party[1] has issued an opinion on biometrics. It identifies various actors that have responsibilities with regard to privacy and biometric systems, and places a strong emphasis on privacy by design at all stages from the manufacture of hardware through to operational deployment.

EU Privacy Law already places a strong emphasis on consent in the collection of personal information. Given New Zealand privacy law's existing EU adequacy status, it is important that we maintain our international reputation.

The Immigration Act 2009 is a useful benchmark to consider. The approach taken to development of that Act's biometric powers recognised the significance of biometric information. It includes a clear framework for the handling of biometric information, including privacy safeguards. It also prescribes that privacy impact assessment be undertaken whenever a power authorising the use of biometrics is implemented.

Virtual and Digital Goods

Customs proposes the option of expanding the definition of "goods" to cover all digital files. Given the rise of the smartphone and cloud computing's ability to pull information into one place, the amount of personal information that people carry around in the form of "digital files" is rapidly growing.

Taken in the context of Customs' proposed clarification of powers to search electronic devices (see below), this could potentially give Customs access to a large amount of personal information. Any option chosen will need to carefully consider how Customs will handle information that is not relevant to Customs' purposes.

Thought should also be given to the wider context of other legislation. The issue of whether digital files can amount to "property" has not been solved, it is the subject of both case law and significant commentary. If Customs chooses to clarify "goods" in its own legislation, thought should be given to any flow-on effects this might have.

Given that extended access powers in the Act would override the Privacy Act, the protections that the Privacy Act affords personal information should be retained. These include ensuring that access is necessary, proportional and reasonable.

Powers

Examining electronic devices

The paper outlines options for facilitating access to information stored on readily-transportable modern electronic devices. We consider that this raises greater privacy risks than has previously been the case.

---

[1] The **Article 29 Working Party** gives expert advice on data protection to the EU and is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. Its name comes from the Data Protection Directive and it was launched in 1996.

We appreciate the need for enforcement agencies to be able to access information held on personal electronic devices in certain circumstances to identify and address criminal offending. However, the privacy risks need to be considered fully before any decisions are made on whether legislative amendments are required, and if so, the form any such changes should take.

As recognised in the paper, electronic devices accompanying travellers may contain extremely personal and sensitive information, both about the individual themselves and others.

Today, the average person crossing the border will carry their lives with them on their smartphone. Providing Customs with the power to examine personal electronic devices could give it access to information such as personal correspondence, banking and medical records – information that until now would have been unlikely to be carried across the border.

Recently we have seen the consequences of handling such information insensitively. Two sisters from Christchurch were detained in Brisbane while the contents of one sister's phone was examined.[2] The resulting public debate this caused stresses the need to approach this issue with care.

The circumstances where such access would be considered reasonable, and the manner in which such access should be enabled must be appropriately circumscribed to ensure against unreasonable intrusions of personal privacy.

Conclusion

We are confident that the review of the Act can result in a legislative framework that enables Customs to meet its objectives, delivers benefits to both business and government, and protects individual privacy.

As this is a discussion document, a number of the more detailed elements are still to be decided. There will therefore be an ongoing need to consider privacy issues as the policy is developed.

The Privacy Commissioner has been pleased with the level of engagement between Customs and OPC on this topic to date. We are committed to an ongoing engagement with this work in future.

[2] Christchurch Muslim sisters horrified by detention at Brisbane airport: http://www.stuff.co.nz/travel/travel-troubles/67711275/christchurch-muslim-sisters-horrified-by-detention-at-brisbane-airport

Useful information

Complaints data

OPC has received 18 complaints regarding Customs since January 2010. Our investigations staff have found Customs to be cooperative and none of the complaints have raised any significant concerns regarding Customs current information handling mechanisms and procedures.

Existing Customs information matches under the Privacy Act

Customs/MSD Arrivals and Departures (commenced 1992)

To identify current clients who leave for or return from overseas while receiving income support payments, and to assist MSD in the recovery of outstanding debts.

Customs/MSD Periods of Residence (commenced 2002)

To enable MSD to confirm periods of residence (here or overseas to determine benefit eligibility.

Customs/Justice Fines Defaulters Alerts (commenced 2006)

To improve fines enforcement by identifying serious defaulters as they cross the border, and to increase voluntary compliance through publicity targeted at travellers.

Customs/IR Student Loan Interest (commenced 2007)

To detect student loan borrowers who leave for or return from overseas so that IR can administer the student loan scheme and its interest-free conditions.

Customs/IR Child Support Alerts (commenced 2008)

To identify parents in serious default of their child support liabilities who leave for, or return from, overseas so that IR can take steps to recover the outstanding debt.

Customs/IR Student Loan Alerts (commenced 2013)

To identify overseas based borrowers in serious default of their repayment obligations who leave for/ return from overseas so IR can take steps to recover the outstanding debt.

Customs/MBIE Motor Vehicle Traders Importers (commenced 2004)

To identify people who have imported more than three motor vehicles in a 12 month period and are not registered as motor vehicle traders.