NEW ZEALAND LAW SOCIETY
NZLS EST 1869

Law Society Building, 26 Waring Taylor Street, Wellington,
DX SP20202, Wellington or PO Box 5041, Lambton Quay,
Wellington 6145, New Zealand

TEL +64 4 472 7837 • FAX +64 4 473 7909
E inquiries@lawsociety.org.nz
www.lawsociety.org.nz • my.lawsociety.org.nz

1 May 2015

Customs and Excise Review
New Zealand Customs Service
PO Box 2218
Wellington 6140

Email: C&EReview@customs.govt.nz

Re: Customs and Excise Act 1996 Review – Discussion Paper 2015

The New Zealand Law Society (Law Society) appreciates the opportunity to comment on the *Customs and Excise Act 1996 Review – Discussion Paper 2015* (discussion paper). Responses to relevant questions are set out below.

Overall Approach

Q2 *What is your view on principles-based legislation, where the detail is in delegated legislation (Regulations, Orders in Council or Customs Rules)? Please give your reasons.*

A regime of statute, regulations and Customs rules can work well, for the reasons outlined in the discussion paper. The Privacy Act 1993 is a good example of such an approach.

Customs is required to manage New Zealand's borders in order to protect the community, to facilitate trade and travel into and out of the country, and to collect revenue. It makes sense for this to be controlled by a principles-based approach set out in legislation, with the detail contained in regulations.

Custom's work raises significant privacy issues, particularly in respect of biometric information and disclosure of information to other agencies. While the detailed mechanics of information sharing and biometric data collection may be appropriately left to delegated legislation (regulations), clear expectations in respect of privacy and biometric data collection should be set out in the primary legislation. It is for Parliament to ensure an appropriate balance between the respective interests is achieved.

However it is not clear that regulations permitting information sharing under Customs legislation are necessary, since there are provisions in the Privacy Act 1993 (Part 9A) which regulate the development of information sharing agreements within and between agencies. No reasons have been given as to why that system is considered inadequate for Customs.

In respect of biometric data, the principles governing the collection and management of such data should be set out in primary legislation because of the importance of the privacy interests at stake (as discussed below). However the procedures and processes for biometric data collection and management could be contained in regulations as long as there remains an appropriate level of scrutiny and oversight.

Q4 *Should Customs prescribe consultation requirements for delegated legislation (Regulations, Orders in Council or Customs Rules) in the new Act? If so, what consultation requirements would you expect there to be?*

The Law Society considers there should be transparency about any impending changes and public consultation, by notice:

- in the *Gazette*,
- in the media where appropriate,
- on the Customs website,
- to the Office of the Privacy Commissioner in respect of any privacy issues, and
- to other relevant persons/groups.

Q5 *What publication requirements would you expect there to be for delegated legislation (Regulations, Orders in Council or Customs Rules)?*

Publication through the Parliamentary Counsel Office and on the Customs website would be appropriate.

Q6 *Should a new Act include a purpose statement?*

Yes, this is a necessary and useful interpretation tool.

Q7 *Should a new Act include a set of principles?*

Yes – see the answer to Q2 above.

Customs' information framework and goals

Comment

Before discussing information principles, it is important to identify the information involved. The discussion paper says that Customs collects information on all goods, people, sea and air craft that cross the New Zealand border. The discussion paper does not explain the full detail of personal information collected by Customs.

In any discussion regarding personal information, it is important to assess the data in light of the Privacy Act principles; for example, is the personal information held necessary for Custom's purposes and lawfully collected? Without such an assessment, it is difficult to analyse privacy harm and risk in respect of the personal information Customs holds and to provide a more meaningful response to the questions posed.

It should also be noted that the European Union expects New Zealand to look after personal information in its jurisdiction and will not recommend trade with New Zealand if New Zealand does not meet international standards on privacy and data protection (see https://www.privacy.org.nz/news-and-publications/statements-media-releases/european-union-endorses-new-zealand-privacy-act-media-release/). Given Custom's mandate in respect of

international trade, it is imperative that Customs works through the personal information issues raised in the discussion paper with the Office of the Privacy Commissioner.

Q8 What are your views on Customs' principles for how we collect, use, store, share and dispose of information? Is anything missing? Should anything be added?

The paper identifies the principles. The Law Society recommends changes (underlined below), to reflect the well-established privacy principles in the Privacy Act 1993 which are based on OECD guidelines:

- Information is only collected, held *(or stored)*, accessed, used and shared for clear, legally supported purposes
- We will be transparent about why we collect information and what we do with that information.
- Information will be collected fairly and lawfully
- the information we collect is protected by appropriate ICT security measures (for example, our servers are built to Government Restricted level) and, for certain levels of information, access is restricted to designated Customs staff
- the information is protected from being unlawfully accessed or hacked, modified or misused
- if the information has been received from another government agency, it is protected ~~in ways requested by that agency~~ in accordance with the law
- the information is protected from inappropriate access or use by users of our system, by the following measures:
    - there must be a clear and lawful purpose for access and sharing
    - people who are granted access are specifically identified and trained, and have the appropriate security clearances
    - access is traceable, audited with clear accountabilities for the access, use, storage and sharing of information
    - Customs carries out frequent risk and security audits (both internal and external) of our information databases
    - Information will be used in a way that is adequate, relevant and not excessive
    - We will ensure an individual's rights to access and correction of their personal information will be met

Q9 What are your views on our goal for our information framework?

The goals stated in the discussion paper are set out below:

"Our goal is to develop a coherent, transparent framework for collecting, using, storing, sharing and disposing of information that:

- *maintains and builds trust and confidence in the way that Customs collects, uses, stores, shares, and disposes information*
- *maximises value for New Zealand from the information that we hold*
- *supports our principles for how we deal with information (see the previous page)*
- *ensures we have flexibility so that we can respond to changes in our operating environment – for example, new technologies and business practices*
- *ensures we receive accurate information and at the right time, preferably in advance*
- *ensures we collect the information we need in the most efficient and effective way."*

The goal of "maximising value for New Zealand from the information we hold" is too vague, is highly subjective and could lead to exploitation of the data. It is also not clear how it fits with the other principles.

The goals should emphasise the protection of personal privacy as a specific goal.

Q10 What are your views on how we should ensure that our information framework aligns with broader government frameworks and initiatives for managing and sharing information?

The Law Society supports alignment with broader government frameworks, with oversight by the Chief Privacy Officer and in consultation with the Office of the Privacy Commissioner, the Office of the Ombudsman and the Chief Archivist.

Information sharing

Q11 What are your views on how our legislative framework for information works now? Do you see any tensions or uncertainty in how we deal with information in general, or, more specifically, with the information that you provide to us?

Managing data and personal information is a complex task, particularly in light of ever-increasing capabilities of technology. The ability of technology to identify data and create access points to that data across large amounts of information (often described as "big data") is significant.

Tensions also arise once an agency holds information, in identifying when an agency must share information, when an agency may share information (or not) and when an agency must not share information. The two boundaries (must and must not share information) are usually straightforward and set out in legislation or through court orders (such as search warrants). The difficulty is when an agency may share information and it either wants to share the information

or does not want to share the information. Often agencies are looking for guidelines in exercising this choice. That can easily be managed through regulations or Codes.

The Law Commission in its inquiry into privacy identified some fundamental points which need to be considered:

Privacy is a subset of two core values:

- Autonomy of humans to live a life of their choosing
- Equal entitlement of people to respect

Privacy can be harmed by the way in which an agency collects, processes and disseminates personal information.

The risks associated with breach of privacy include: injustice; loss of personal control over information; loss of dignity (embarrassment) by disclosure of information; and loss of public confidence and trust.

It appears from the discussion paper that Customs wishes to maintain public trust and confidence, but also wants significantly greater powers to share information with enforcement agencies, particularly the Police. Those agencies would presumably welcome direct access to Customs' databases without having to go through the usual legislative or court processes for seeking the information. The rationale for such information sharing is that in order to protect New Zealand, government agencies need to understand potential risk through sharing multiple pieces of information to develop a richer picture of risk which will not come from one agency's information system.

However, without more detail about the information held by Customs, it is difficult to assess the potential privacy risks and harm posed by the proposals. The rationale for agencies having direct access to information held by Customs needs to be supported by more evidence and analysis. For example, the travel details of a couple having an extramarital affair will be highly sensitive and confidential to that couple, but it is not clear if Customs has information on people travelling together. Similarly, the personal information of a person experiencing a bi-polar event in-flight is highly sensitive but it is not clear if that information is passed from an airline to Customs.

The discussion paper gives an example of a person using cash to buy a ticket to travel to New Zealand two days before travel. This might indicate criminal activity, or it might simply indicate rushed travel plans due, for example, to a death in the family. The suggestion appears to be that every time a traveller pays with cash, this needs to be referred to the Police. If the Police have concerns about a person, direct access to Customs' databases might provide information that, in combination with other information held by Police, might suggest criminal activity. However it is not clear why usual access requests or an information sharing agreement would not suffice. Direct access by the Police also risks inviting unnecessary fishing expeditions into personal information held by Customs.

This scenario has the potential to place a significant burden on either Customs or the Police. In addition it is not clear whether Customs would be expected to maintain surveillance of its data for potentially criminal activity, or whether that would be the responsibility of the Police. Nor is

it clear which agency would be held accountable for overlooking information that would have indicated criminal activity such as a child abduction.

Another example in the paper is that Customs knows the travel details of an arms dealer, such information being immediately helpful to the Police. It is not clear why there would currently be any delay to this information being provided through access under anti-terrorism legislation, a request under the Official Information Act or through an information sharing agreement under the Privacy Act.

This example also refers to appropriate training and security clearance, but what constitutes "appropriate" training and security clearance is not explained.

The discussion paper rightly places much emphasis on transparency. However there is likely to be a negative impact on public trust and confidence if:

- Customs develops a reputation as a conduit of information for law enforcement agencies such as the Police, or
- the agency receiving the information has poor information handling and security processes.

As already noted, the discussion paper does not explain why Customs, in respect of New Zealand agencies, does not simply implement an information sharing agreement under Part 9A of the Privacy Act. The purpose of Part 9A (s 96A) is to enable the sharing of personal information to facilitate the provision of public services. The Act provides a mechanism for the approval of information sharing agreements between or within agencies and deals with any necessary exemptions or modifications to the information privacy principles.

This is particularly important as the discussion paper identifies that uncertainty around information sharing is the main concern. Section 96A(2)(c) of the Privacy Act states that Part 9A information sharing agreements reduce "… any uncertainty about whether personal information can be lawfully shared for the provision of … public services".

If the intention is that an information sharing agreement not be put in place, then more information would be needed to assess the proposals, such as:

- What information is to be available and for what purposes?
- Who has access and in what circumstances?
- What are the operational details such as:
    - How is access authenticated?
    - What security steps are in place for transfer of data?
    - What are the arrangements for security within each agency?
    - How long can the agencies retain the data?
    - What are the mechanisms (tracking, audit etc) to ensure that access happens as regulated?
    - Are there any costs?
- What privacy safeguards have been put in place such as:

- What happens if the data is inaccurate?
- Can an individual request confidentiality in special circumstances? If so, who decides?

- How is the public to be informed of the access and their rights to access and correction of their own information?
- Which agency is responsible for an interference with privacy complaint?

Q14 Should Customs share information with government agencies for broader government purposes beyond border protection? Please give your reasons.

In the discussion paper there are examples of sharing for broader government purposes. All of the examples appear to be well managed under current arrangements.

Receiving and accessing information

Protections for travel records

Q25 What protections do you think should be required for Passenger Name Record information?

It is difficult to answer this question without knowing the personal information Customs is seeking to retain under the new "push" system.

The privacy enhancing response is to maintain the 14 days prior to travel "pull" access to information, with a search warrant required for information outside that period. Once information is received under the new push system, Customs would need to identify the minimum information it wishes to retain for the purposes of international law enforcement and to be transparent about that purpose.

Biometric information

Q29 Do you agree with Customs' proposal that our legislation should explicitly recognise that Customs needs to access, collect, use, and share biometric information to carry out our functions? Please give your reasons.

It is accepted that identification of people is significantly assisted by biometric information. It is also accepted that Customs needs to maximise certainty with respect to identification. However the following points are noted:

- The collection and use of biometric information must be transparent, using a 'privacy by design' approach (i.e., an approach to protecting privacy by embedding it into the design specifications of technologies etc.).
- The initial collection of biometric information must be accurately matched to the correct person.

- It is important to recognise that because of a person's particular presentation (such as bad fingerprints or disfigured facial features), some biometric information cannot be recorded. This could lead to disability discrimination if such a person is refused services as a result.
- There needs to be testing for accuracy and error rates.
- The minimum amount of biometric information necessary for identification in specific circumstances should be clearly defined.
- Clear policies are needed around use and disclosure. In particular, automatic access to this data by Police needs to be carefully assessed. Citizens do not have to provide their fingerprints to the Police unless under arrest. That right should not change just because a citizen has crossed a border. Giving Police direct access to the database would circumvent that right.
- The use of biometrics should comply with principle 12 of the Privacy Act and not become a "unique identifier" across agencies.
- Privacy impact assessment and transparency are necessary if biometric information collected is to be used for another purpose.
- The security of the information collected should be ensured.

Q31 Do you think Customs' access to, and collection, use, and sharing of biometric information requires additional protections above those in place for other types of personal information? If so, what further protections do you think there should be?

As biometrics involves health data, Customs must meet all security standards and protocols (see National Health IT Board: http://healthitboard.health.govt.nz/standards).

Virtual and digital goods

Q33 What do you think is the best option to address the gaps that have been identified? What are your reasons?

The best option is for regulations to prescribe the digital files which are covered. This would ensure ongoing and appropriate oversight of the implementation of the legislation and its principles. This should not be left to Customs' discretion.

Q34 Are there other issues around the cross-border transfer of digital files (other than revenue issues) that are not considered in this section and that you believe should be considered?

Yes. It is important that any cross-border transfer of information complies with the New Zealand Privacy Act.

Electronic devices

Q93 Do you think the new Act should explicitly include electronic devices in the scope of Customs' routine baggage search powers at the border? Please give your reasons.

The discussion paper says the ability to search paper records should extend to searches of electronic devices. Electronic devices may contain intimate, sensitive and secret personal and commercial material: diaries, meeting records, purchases, correspondence, notes, photos, "selfies", other photos, film clips (any of which could be extremely intimate and/or embarrassing), drafts and deleted material, other transaction records, and so on. They may also contain legally privileged and/or confidential material.

It appears that Customs already has wide powers in respect of searches of electronic devices in order to detect objectionable material and evidence of offending, such as evidence of illegal drugs being brought across the border.

A search of electronic devices will involve looking for potentially incriminating evidence or information, such as:

- travel documentation (e.g. how a ticket was paid for, where the ticket was booked and issued, the class of travel, or any unusual travel routes)
- objectionable images
- evidence of offending against the Customs and Excise Act (such as importing prohibited items)
- verifying the value of dutiable goods through electronic receipts or invoices

The scope of a search of electronic devices is not clear from the discussion paper, nor whether it is possible to avoid viewing private information or images (such as intimate pictures) that are irrelevant to the search for objectionable material.

The paper refers to Customs officers "knowing" there is illegal content or content which would support commission of an offence (although how a Customs officer "knows" that is not explained). The typical evidential foundation for such knowledge could inform a threshold for a preliminary search.

The Law Society suggests there should be two thresholds for a search: one for the preliminary search and one for the forensic analysis, which should depend on what is found in the preliminary search.

It would be helpful to understand how people are currently informed of their rights – such as their right to refuse a search when there is no foundation or their right to assert privilege over electronic content.

It will also be necessary to make provision for a review process, where exercise of the powers can be challenged, to ensure there are safeguards to prevent any abuse of the powers (for example, where there appears to be a campaign to target journalists or activists).

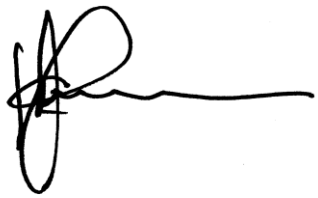
The discussion paper at page 135 notes that explicitly including electronic devices in the scope of routine baggage searches "… is consistent with similar powers available to customs agencies in Australia, Canada, the United States and the United Kingdom. *However, developing law in other countries is beginning to place greater weight on the privacy implications associated with information contained on electronic devices, including at the border*" (emphasis added).

The paper does not provide details about this developing law but it is clearly an important factor that requires serious consideration.

Conclusion

If you wish to discuss these comments, please do not hesitate to contact the convenor of the Law Society's Human Rights and Privacy Committee, Dr Andrew Butler, via the committee secretary Vicky Stanbridge (04 463 2912, vicky.stanbridge@lawsociety.org.nz).

Yours sincerely,



Chris Moore
President