NEW ZEALAND LAW SOCIETY

NZLS EST 1869

Customs and Excise Bill

13/02/2017

Customs and Excise Bill

1 Overview

1.1 The New Zealand Law Society welcomes the opportunity to comment on the Customs and Excise Bill (the Bill).

1.2 The Law Society acknowledges that this is an important opportunity to update our border legislation, to take account of the developments in technology, trade, security and operational practice since the current Act was passed in 1996. Opportunities for updating such major pieces of legislation do not occur frequently. The Law Society's comments are therefore aimed at making sure that the Bill remains fit for purpose for some time to come.

1.3 The Law Society's recommendations focus on some general areas of the Bill where improvements appear to be practicable and desirable:

1.3.1 It is possible to make the Bill clearer about the purposes for which Customs may collect **biometric information**. Clause 182 of the Bill should include a requirement for Customs to inform an individual when it is voluntary or mandatory to provide biometric information, and to inform them what will happen if they refuse the collection of biometric information.

1.3.2 The Bill should include further **reporting requirements** regarding use of the detention powers and collection of biometric information.

1.3.3 The current version of the Bill provides some useful clarity around **information sharing**, and the purposes for which it can occur. However, further protections are required to ensure that information sharing occurs in a transparent and accountable way. It is also important to make it clear when the information privacy principles in the Privacy Act will continue to apply.

1.3.4 While the Law Society accepts that **searches of electronic devices** are often appropriate, it continues to have concerns about the scope of some of the search and seizure provisions. Those concerns include the need to ensure other forms of privilege are protected, the need for backstop protections for privacy in situations where sensitive personal and confidential material is stored on devices, and the lack of clarity about how the search, identity and document retention provisions interrelate.

1.3.5 **Indecent or obscene articles** (clause 95(1)(b)) are not defined in the Bill. This creates unhelpfully wide room for administrative discretion to seize or prohibit information, with consequent impacts on freedom of expression. The Law Society recommends that clause 95(1)(b) should be clarified and narrowed, or deleted.

1.3.6 The ability to **prohibit the import or export of documents and electronic documents** "in the public interest" (clause 96) has potentially serious implications for freedom of expression. The Law Society recommends that the scope and purpose of the provision should be clarified and narrowed.

1.3.7 Clause 275, relating to **automated decisions**, is so widely worded as to be unclear. To the extent that it relates to use of systems such as SmartGate for efficient passenger processing, the reference appears unobjectionable but the provision is potentially much wider and could apply to decisions that significantly affect people's rights. The Law Society recommends that the scope and intent of the provision should be clarified, and additional protections added.

1.3.8 The Law Society recommends that the Bill should ensure that people have access to a clear process to **correct inaccurate information** about themselves, and should expressly require that any corrections made to personal information are forwarded to other agencies (whether domestic or overseas) to which the original, incorrect information was sent.

2 Biometric information

Definition of "biometric information" (clause 5)

2.1 Biometric information is generally viewed as highly sensitive, and therefore requires particularly careful controls. The Law Society agrees that Customs will often need to collect biometric information, including in situations where it is necessary to verify an individual's identity. It has no concerns about the definition of biometric information contained within the Bill. The listed identifiers are internationally accepted, are proved to be effective and are not disproportionately intrusive.

2.2 The Law Society notes that the definition of "biometric information" should continue to be regulated at the statutory level (not in regulations or administrative processes). New biometric technologies will emerge over time, but each should be subjected to Parliamentary scrutiny to ensure that they return sufficiently accurate results and do not have a disproportionate effect on individuals.

Extension of collection to those departing New Zealand (clause 53)

2.3 The Law Society accepts that there is a case to be made for collecting biometric information as an individual leaves New Zealand, not only when they enter New Zealand. This will assist New Zealand to meet its international obligations, and may also provide additional assurance to relevant domestic authorities, such as MBIE (Immigration).

2.4 However, the Law Society recommends that the Bill should limit the purposes for which biometric information collected on departure may be retained, used or disclosed. The current purposes are too broadly stated and unclear. They leave open the possibility that Customs could simply act as a general collection agent for a foreign authority under the heading of "border security". Adding in some further limitations will help to assure individuals that their information will not be misused or disclosed to those who are not entitled to receive it.

Consistent clauses about collecting biometric information

2.5 Clause 53 does not currently expressly allow Customs to collect biometric information for the purpose of verifying a person's identity. Instead, that power is contained in clause 182, which allows for collection of biometric information for the purpose of identifying the individual using biometric matching.

2.6 To some extent, identity verification is likely to be implicit in the clause's purposes of passenger processing, monitoring persons and border security. However, it would be clearer if the clauses were either located together in the statute or if clause 53 were amended to allow Customs "to collect biometric information for identity verification purposes as specified in clause 182".

Notification of rights (clause 182)

2.7 Clause 182 of the Bill currently states that a Customs officer may 'request' biometric information. However, it is likely that individuals will be under the impression that they are *compelled* to provide the information, unless they are told otherwise.[1] It is important that people are expressly informed when information collection is voluntary, to avoid misunderstandings. If collection is mandatory, it should be made clear which statutory provision applies. In either case, Customs should be required to specify the consequences of failing to provide the information.

2.8 The Law Society recommends that clause 182 should be amended to require Customs officers to provide people with this additional information. This will ensure that the legislation fully mirrors the rights in principle 3 of the Privacy Act and leaves no room for misunderstanding.

3 Additional reporting requirements

3.1 Reporting provides a useful basis to assess the effectiveness of the legislation, and to provide assurance against misuse of the very significant powers that it contains. The Bill contains some useful reporting requirements in relation to searches of electronic devices and use of force, which the Law Society supports.

---

[1] See for instance https://www.newshub.co.nz/new-zealand/2017/01/police-using-misleading-forms-to-gather-information.html, in which the Police have had to review their forms to avoid any misleading suggestion that agencies are compelled to give information to the Police.

3.2 However, the reporting requirements could go further. In particular, it would be useful for Customs to be required to report statistical information on age, gender and ethnicity of those who are detained using powers under this Bill. This would enhance transparency and accountability, including providing oversight agencies such as the Ombudsmen or Human Rights Commission with additional information that could assist with their enquiries.

3.3 Similarly, specific reporting on collection, use and disclosure of biometric information could assist in enhancing trust in that aspect of Customs' system.

4 Information sharing

4.1 There are three principal information sharing models proposed by the Bill.

Information matching programmes

4.2 The first (clauses 284 – 288) re-enacts existing provisions relating to information matching programmes, which are governed by part 10 of the Privacy Act. The Law Society has no objection to these provisions. It is efficient to maintain existing programmes that have been found to work well. The Privacy Commissioner also has formal oversight over the operation of all part 10 information matching programmes, which provides an important protection.

Direct access arrangements

4.3 Direct access arrangements can provide easy, timely and efficient mechanisms for obtaining and disclosing information for legitimate and controlled purposes. However, such arrangements raise two significant issues.

4.4 The first is that direct access arrangements should not provide an agency with a back door method of obtaining information that it would usually get only through using a specified legal process. One obvious example is that the Police should not be able to get direct access to information (particularly highly sensitive information) for which it would normally require a warrant, a production order or another legal power to obtain. The Law Society has previously made this point in its submission to Customs as part of the public consultation phase of this legislative review, and as part of its submission on the Enhancing Identity Verification and Border Processes Legislation Bill, currently before Parliament. The way in which clause 293 is worded provides little certainty that appropriate protections will be in place.

4.5 The second point is that direct access arrangements should be accompanied by strict requirements for audit and reporting, so that the validity of the access can be confirmed, the operation of the programme is transparent and steps can be taken to address any overreach. These requirements could be added to clause 293.

Information sharing agreements

4.6 For other regular information sharing needs, the Bill proposes that Customs should be able to enter agreements at an administrative level with other agencies (clause 294).

4.7 It is unclear whether those agreements are in the nature of MOUs, which do not override existing legislation but would require Customs and the other agencies to comply with the Privacy Act provisions as normal. If this is the case, they may be unproblematic, although given the sensitivity of much of the information, and the fact it will often be negative information about individuals, it would still be valuable to amend the Bill to insert some further accountability and privacy protection mechanisms as discussed below.

4.8 However, if the agreements are intended to override the normal protections in the Privacy Act, the legislation should make this clear, and any override must be clearly justified (which it currently is not). It is also vital that the legislation is amended to provide further protections for individuals.

4.9 Customs appears to have rejected the possibility of using the Approved Information Sharing Agreement (AISA) framework in part 9A of the Privacy Act, which is a balanced framework that allows agencies to perform their public functions but also ensures appropriate levels of protection of personal information. The RIS[2] suggests that the basis for this rejection is that the information to be shared will not only be personal information, but also non-personal information including commercially confidential information.

4.10 The Law Society supports Customs' desire to protect confidential commercial information. In addition, it recognises that it often makes little sense to develop separate systems or arrangements for handling personal and non-personal information that is collected, used or disclosed for the same purpose. Attempting to do so can be confusing for both officials and the public.

4.11 There is however no reason why an AISA cannot also be drafted to cover non-personal information. An AISA cannot change the agency's *legal* obligations in relation to non-personal information (unlike in the case of personal information, where an AISA can be used to expressly override several of the privacy principles). However, this does not prevent an agency from using the same document to cover all relevant types of information. Many of the protections that were designed to apply to personal information would also provide useful protection for confidential commercial information and could therefore support the result that Customs wishes to achieve. The insistence in the RIS that an AISA cannot work in these circumstances is therefore puzzling.

---

2 *Customs and Excise Act review: managing and disclosing information*, 8 September 2015, http://www.customs.govt.nz/news/resources/customs-and-excise-act-review/Documents/CandEAct1996Review-Information%20Management%20and%20disclosure%20RIS.pdf

4.12 However, if it is seen as preferable to use the Customs Bill as the basis for developing these information sharing arrangements, then the Law Society recommends that the Bill itself needs to set out all the necessary protections that govern the arrangements. Unlike an AISA, the process as set out in the Bill does not require Cabinet approval or an Order in Council, and would not be subject to Parliamentary scrutiny by the Regulations Review Committee. The usual important levels of oversight and transparency are therefore missing. As a result, the primary statute needs to set out the required framework that each agreement must follow.

4.13 The Bill in its current form goes part way towards doing so. For instance, clause 294(4) specifies that an agreement must set out the information that can be shared, the purposes for which it can be shared, the safeguards that will apply and the circumstances under which the information can be disclosed.

4.14 The requirement to consult with the Privacy Commissioner is also important, and must be retained in the Bill. However, consultation is insufficient on its own to guarantee that the agreements will operate in a proportionate and justifiable manner. The Commissioner has no power of veto, and there is also no specific requirement for him to report to the Minister or publicly on such arrangements. Again, the context is important, particularly the fact that the information that is shared will often be sensitive or negative about the individual.

4.15 To address the issue, the Law Society recommends that certain key protections should be included in the Bill. In particular, it is important to include provisions requiring Customs to:

- undertake a privacy impact assessment in relation to each agreement that involves personal information, to ensure that any risks and appropriate mitigations are properly identified;
- perform a cost/benefit analysis to make sure that the agreement will be effective and cost-efficient;
- set out in the agreement what steps will be taken before adverse action is taken against a person;
- identify what complaints process people can use, and what remedies are available if an agency breaches the agreement;
- consult on an agreement before finalising it;
- report regularly on its ongoing operation;
- make the agreement available for public view on Customs' website.

5 Searches of electronic devices (clause 207)

5.1 The Law Society accepts that searches of electronic devices by Customs are appropriate. It also welcomes many aspects of the proposed constraints relating to the searches. Examples include the search thresholds, the limited reasons for searches, the controls on searches, the protection of legal professional privilege, and the requirement to report the number of searches to Parliament.

5.2 However, the Law Society continues to have concerns about this provision. In particular:

5.2.1 Both forms of search (initial and full) seem to permit access to everything on the device, despite the fact that extremely sensitive personal and confidential material may be stored on such devices. The Law Society submits that there needs to be further guidance, in the form of subsidiary legislation, including supervision and a complaints regime (allowing the exercise of the powers to be challenged), to govern the content and conduct of such searches to ensure that any privacy infringements are minimised as much as is possible in the context of a search.

5.2.2 Legal professional privilege is protected (clause 233), but no other privilege recognised in section 136 of the Search and Surveillance Act 2012 is protected, including journalistic privilege, informers' privilege, and medical and religious privileges. This is a serious issue, especially as the Bill provides a greater ability for Customs information to be shared with other agencies. It is unclear why the other privileges are not recognised and protected in this context. It is also inconsistent with the rest of the Bill, which routinely adopts subpart 5 of Part 4 of the Search and Surveillance Act, recognising these privileges: see clauses 170, 189, 190, 193, 200, 216 and 221.

5.2.3 There should also be an explicit process to provide a proper opportunity for privileges to be asserted. Passengers should also be told of the reasons for any search. Furthermore, as with collection of biometric information, Customs should not be permitted to conduct any searches on the basis that they are voluntary, without an explicit warning to passengers that they are not required to provide their devices for search.

5.2.4 Collection of irrelevant material through such searches is inevitable. Controls are therefore required to ensure that irrelevant material is not kept, used and disclosed to others. The Law Society recommends that any material copied should not be available for disclosure under the new information management regime, except for the purposes of dealing with the identified relevant offending.

5.2.5 The relationship between the provisions governing searches of electronic devices (clause 207), the provisions allowing Customs to demand identity documents, including documents

contained on a device (clause 180), and the provisions governing retention of documents (clauses 235 – 238) is not clear. Under clause 180, it seems that if a relevant document is on an electronic device, it must be opened (using a password, although this is not stated) and the device handed over for inspection and possible retention. The definition of "document" includes a device storing a document (clause 5). Under clause 180, the document on the device must be examined briefly and then the device returned, unless exceptions apply (clauses 235 and 238). These contemplate the document being kept, and therefore apparently permit the device to be kept. It is not clear why simply taking a photograph of the document on the device would not suffice. Under clause 235, the owner of the document is entitled to a "certified copy" if it is detained. That does not make any sense in the case of a device. Moreover, clause 180 allows the device to be kept for as long as reasonably necessary while Customs decides whether to retain the document under clause 235. But clause 180 applies the thresholds in clause 207, which relate to reasonable cause to suspect or believe that material is present pertaining to relevant offences. This presupposes that clause 180 permits examination of further material on the device besides the identity document. The Law Society recommends that the relationship between these clauses be clarified.

5.2.6 It would be useful for the report to Parliament to include information about how many of the searches produced information that led to relevant prosecutions and convictions.

6 Indecent or obscene articles (clause 95)

6.1 Clause 95 prohibits import and export of objectionable publications, as defined under New Zealand's censorship laws (see clause 5). The Law Society agrees that it is appropriate for Customs to have this power.

6.2 However, clause 95(1)(b) also prohibits importation of "all other indecent or obscene articles". That term is not defined and is not linked to definitions in the censorship legislation. It is obviously intended to refer to a wider class of articles, but its scope is uncertain. As the provision stands, it appears that it would provide Customs officials with a wide and potentially highly subjective discretion about the types of articles that come within this category. It is also apparently acceptable to export that wider class of article (clause 95(2)), but not to import them (clause 95(1)), although the reason for the double standard is unclear.

6.3 A power to prohibit import or export of material has the potential to impact significantly on freedom of expression. The scope of and justification for the limitation should be clear. The Bill

currently does neither. Instead, the phrase harks back to obsolete provisions in the old Indecent Publications legislation.

6.4 In the absence of any proper justification for its inclusion, and additional provisions defining the types of articles covered and stating who is able to determine what is and is not "indecent or obscene", clause 95(1)(b) should be removed.

7 A prohibition on use of the internet for certain purposes? (clause 96)

7.1 A related point is that clause 96 allows the Governor-General by Order in Council to prohibit the import or export of goods – which now includes documents and electronic documents (clause 96(11) and (12)) – when the Minister considers this necessary in the public interest.

7.2 Importation is defined to include: "in relation to prohibited imports that are objectionable publications or other indecent or obscene articles **or other documents**, **includes their transmission by any means** (other than by broadcasting) into New Zealand from a point outside New Zealand" (emphasis added). There is a similarly expansive definition for exports (although this omits reference to indecent or obscene articles, it includes "other documents").

7.3 This clause plainly includes sending or receiving an emailed document, and apparently even includes posting or accessing material online. The provision does not appear to be restricted to documents with a commercial value, such as books. Again, this raises significant free speech issues, given the width of the Minister's power. Furthermore, it is not clear how Customs' extensive powers apply in this situation.

7.4 The Law Society therefore recommends that the scope and purpose of this provision be clarified and narrowed.

8 Automated decision making (clause 275)

8.1 Clause 275 states the "The chief executive may approve the use of automated electronic systems by a specified person to make any decision, exercise any power, comply with any obligation, or carry out any other related action under any specified provision."

8.2 To the extent that the clause is intended to refer to use of systems such as SmartGate for efficient passenger processing, the reference appears unobjectionable, as long as the requirement to have a human decision maker also available remains in the Bill (see clause 275(2)(c)). It is also sensible for the provision not to refer to specific types of technology as this will ensure that the provision has greater longevity.

8.3 However, the effect of the provision is potentially extremely wide. It could theoretically apply to the exercise of any of Customs' extensive powers or the making of any of its decisions. Many of those powers and decisions significantly affect people's rights.

8.4 The controls provided for in the Bill are helpful – that Customs needs to be in control of the system (clause 275(2)(a)), that the Chief Executive needs to be satisfied that the system has the capacity to do the task reliably (clause 275(2)(b)), that the Privacy Commissioner must be consulted (clause 275(4)) and that details about the automated system must be published (clause 276). However, the technical capability of an automated system to make a reliable decision does not always mean that automated decision making is *appropriate*, particularly when the effect on individuals is lasting and significant. Even though an official may vary a decision made by an automated system, they are not required to do so (clause 277).

8.5 The Law Society therefore recommends that the scope and intent of the provision should be clarified. It also recommends that a provision should be added to clause 275(2)(b) requiring the Chief Executive to be satisfied that use of the automated electronic system is appropriate and not disproportionate in the circumstances, given the effect of the decision on the interests of affected persons.

9 Accuracy of information

9.1 The Law Society notes that the Bill does not include a process for people to follow if Customs holds inaccurate information about them, or that enables them to obtain redress. Instead, it appears to rely on the duty under the Privacy Act for an agency to take reasonable steps to check that information is accurate, relevant, up to date and not misleading before it uses that information (principle 8). The Privacy Act also provides people with a right to request that an agency correct personal information about them (principle 7) and to advise other agencies of that correction.

9.2 The rights in the Privacy Act are strong and generally effective (although, anecdotally, it is not always clear whether information corrections are notified to other agencies to which that information has been passed in the meantime). However, it only covers information about individuals, not information about legal persons (there is a correction right in section 26 of the Official Information Act, but it is more limited). Also, inaccurate or misleading information held by Customs can have a particularly significant impact on individuals, including on their freedom of movement. The move to greater information sharing with other agencies also increases the risk that incorrect information will be perpetuated in other agencies' systems and decision making processes.

9.3 The Law Society therefore recommends that the Bill supplement the existing rights in the Privacy Act and Official Information Act by explicitly addressing the issue. Provisions should be inserted to require the Chief Executive to ensure there is a streamlined process for making correction requests (for both natural and legal persons) and for providing efficient and timely responses to those requests; and to ensure that where information is corrected, other agencies to which that information has been disclosed must be informed of the correction.

10 Conclusion

10.1 The Law Society would welcome an opportunity to be heard in support of its submission.

Kathryn Beck
President
13 February 2017