TECHNOLOGY AND DIGITAL GOODS

AT A GLANCE

Advances in technology have meant that Customs has had to continually adapt to ensure we can effectively respond to threats at the border and facilitate trade and travel.

One of the key goals for this review is to ensure that Customs' legislation is future-proofed so that it can adapt to changes, particularly technological advances.

Getting your feedback

We would like your views on the following issues and proposals:

- the need to clarify Customs' role in managing biometric information for Customs purposes
- the need to clearly define the digital files that Customs can intercept at the border
- whether businesses should be allowed to store their business records offshore if they have Customs' prior approval.

Since the current legislation, the Customs and Excise Act 1996, was introduced, technology has advanced far beyond what was thought of in the mid-1990s. Business is now conducted mainly online and through electronic devices, and people now deal with significant portions of their lives on electronic devices.

Customs has been adapting our capabilities and driving changes in our legislation to support these technological advances. This is both to ensure that we can operate efficiently alongside wider supply chains for trade and travel, and so we can perform our functions effectively.

We know that technology will continue to advance, and we want to make sure Customs' legislation allows us to adapt to and make use of these advances without having to amend the legislation. The three areas of technology that we think will expand further in the coming years and that require our attention are:

- biometric information, and how Customs collects and uses it
- virtual and digital goods, and how we manage them at the border
- alternative methods for storing business records.

These areas are discussed further in the following pages.

Biometric information

We are considering whether our legislation should include clearer authority for Customs to collect, access and use biometric information. We think that this would clarify our present legislative authority to manage biometric information for Customs purposes and general law-enforcement purposes. It would also allow us to accommodate future potential changes in the use of biometric information to manage the security of the border and to facilitate people crossing the border.

As we discussed earlier in this paper (see page 31), Customs' goal for how we manage information (including personal information) is to develop a coherent, transparent framework for the collection, use, storage and management of information that, among other things:

- maintains and builds trust and confidence in the way that Customs deals with information
- maximises value for New Zealand from the information that Customs holds, particularly for better protecting New Zealand and growing the economy, and
- supports our principles for information (see page 30).

We want to more clearly provide for biometric information in our information management framework.

Customs does not intend to create any additional computer infrastructure to store biometric information. The Government has invested in Immigration New Zealand and the Department of Internal Affairs to be lead repositories of identity information, including biometric information. Customs does not intend to replicate or replace those systems.

Terms used in this chapter

Biometric information: information about an individual's physical or behavioural characteristics that can be scientifically measured, most commonly including a facial image, fingerprints, iris scans, DNA profiles, and finger and palm prints.

SmartGate: an automated border-processing system that gives certain electronic passport holders the option to self-process through passport control when arriving at and departing from New Zealand international airports. SmartGate uses the electronic information held in an electronic passport and facial recognition technology to verify the identity of the passport holder for Customs and Immigration purposes.

Customs does not intend to duplicate in the Customs and Excise Act any uses for biometric information for traveller processing that are already covered by the Immigration Act.

We also do not intend to extend the types of biometrics collected beyond those currently used in traveller processing. Immigration New Zealand would lead any changes to the types of biometrics required for foreign nationals, and the Department of Internal Affairs would lead

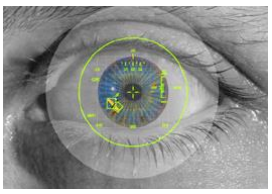
any changes to biometrics in New Zealand passports. Changes are not currently on these agencies' agendas.

Biometrics and their use

Biometric information is becoming an increasingly common way of establishing or confirming a person's identity. Inland Revenue, for example, has over one million subscribers to its voice recognition programme, and new generation smartphones can be locked and unlocked using a fingerprint.

A number of different biometrics are already in wide use, and new and emerging biometrics range from DNA to voice and vein patterns. The most relevant biometrics in the border context are:

Face – currently the most widely used internationally for traveller processing



Eyes – iris or retina recognition

Fingerprints and palm prints

Biometric information is more accurate and reliable than traditional methods of verifying identity, such as simply looking at a photo or signature. Biometric information that is encrypted and stored on an electronic chip inside a passport is more secure than information recorded on traditional passports, and it reduces the risk of identity theft and passport fraud.

How Customs currently uses biometrics

Customs' authority to use and collect biometric information (currently biometric photographs incorporating facial recognition technology) derives from the Customs and Excise Act, several other different pieces of legislation, and under arrangements with other government agencies whom we work on behalf of at the border.

Our largest source of biometric information is from processing travellers for customs purposes and for immigration purposes when acting as Immigration officers, through SmartGate. A traveller can use SmartGate as an alternative option to being processed by a Customs officer. The SmartGate technology compares live facial images with biometric images on electronic chips in the passports of eligible travellers.[6] This automated processing enables us to process large numbers of travellers quickly, enabling a faster and more reliable means of identifying people of interest to Customs.

[6] Currently these are Australian, New Zealand, United Kingdom, United States and Canadian electronic passport holders. More nationalities will be added over time.

Developing and future uses of biometrics at the border

Worldwide, more biometric-compatible passports (that is, those with an electronic chip), conforming to international standards, are coming into circulation. Advances in technology are also allowing biometric information to be collected from a wider range of travellers, including from those holding non-electronic passports. More sophisticated automated systems are also being developed around the world that can accept electronic passports from different countries and with different types of biometric information.

As technology advances, government agencies are looking to use additional and multiple biometrics to provide greater certainty of people's identities. Systems that rely solely on facial biometrics, for example, are subject to some obvious limitations: people wanting to defeat the system can change their appearance or use the passport of someone who looks very like them (twins or other siblings for example), and the appearance of legitimate travellers will of course simply change over time.

Biometric information at the border of the future

In addition to facial images, Immigration New Zealand can also collect fingerprints and iris scans from foreign nationals when they arrive and depart. However, it does not currently have the capability to collect iris scans, or share these with domestic or overseas partners.

Agencies that Customs represents at the border could collect the biometric information of people of interest and share this information with Customs. Customs may then use that information to identify and intercept these people at the border. Customs needs the capability to respond to that information.

What other countries do at the border

Australia, which also uses SmartGate technology, keeps biometric information (photographs incorporating facial recognition technology) collected at the border for seven years, so that the information can be matched against travel records and accessed as needed for law enforcement purposes. The photographs and biometric templates must also be kept as evidence of the grounds on which the traveller was cleared across the border.

The United States records all fingerprints and a photograph of foreign airline passengers visiting the United States (except Canadians), keeping it in databases for 75 years for border management and control purposes. The United States also plans to test a biometric programme on departure soon. A voluntary joint Canada-United States program uses iris recognition biometric technology.

Proposed European Union regulations would require Member States to use fingerprints and a photograph for immigration purposes. The European Union currently stores biometric information (mainly fingerprints) of foreign national visa applicants for five years.

Biometrics: The law as it stands

Biometric information falls within the definition of "personal information" in the Privacy Act 1993. The use of biometrics is also explicitly authorised under the Immigration Act 2009 and the Policing Act 2008. In the Immigration Act, biometric information (defined as including head and shoulder photographs, fingerprints, and iris scans) may be used to establish or verify a person's identity or assist in immigration-related decisions. In the Policing Act, biometric information (defined as including DNA profiles and finger and palm prints) may be used to match prospective Police employees against other information held by the Police.

The Customs and Excise Act currently allows Customs to use biometric photographs incorporating facial recognition technology provided by SmartGate to confirm the identity of eligible travellers for Customs and Immigration purposes. Travellers' use of SmartGate to verify their identity on arrival and departure is voluntary, as an alternative option to manual processing.

> In 2014, 71.7 percent of SmartGate users were New Zealanders

As designated Immigration officers under the Immigration Act 2009, Customs officers can also collect and use biometric information from arriving and departing foreign nationals in order to confirm their identity. However, there is no clear equivalent authority to require this information from New Zealanders when they arrive and depart. There is an opportunity to simplify Customs' collection, use, access to and sharing of biometric information, similar to our collection of other personal information and use of facial recognition technology in SmartGate.

Our information-sharing arrangements with key agencies that collect biometric information allow us to access these agencies' biometric information when authorised so that we can investigate Customs offences. To increase transparency, the Act should give Customs clearer authority to collect biometric information for our own purposes and to share that information with other agencies for law-enforcement purposes.

The opportunity to provide for Customs' use of biometrics

Protecting New Zealand at the border through intelligence-led, risk-based border management, and as part of the law enforcement community, means that accurately verifying the identity of both New Zealanders and foreign nationals matters to Customs.

Customs' role at the border also means that we need to be able to effectively perform tasks on behalf of other agencies by being able to receive and share biometric information with them. Customs' role is to assess risk across all travellers, regardless of nationality or immigration status. Our use of the biometric information authorised by the Immigration Act covers only part of Customs' wider border security functions.

There is an opportunity to consider how long biometric information is stored. Technology is providing opportunities for biometric information to be used beyond immediate traveller processing purposes. This could include real-time matching of images, converting still or

closed circuit television (CCTV) images to a biometric form, and sharing biometric photographs of persons of interest from Customs investigations with other agencies to establish or confirm their identity.

Customs would not be able to take full advantage of these opportunities if we could not retain access to biometric information for a reasonable period of time to investigate possible offences against our Act and other legislation that we enforce at the border.

Examples of potential Customs uses of biometric information beyond those authorised by the Immigration Act

Customs currently uses manual processes in trying to identify and intercept unidentified criminals at the border. For example, Customs officers at airports manually compare travellers with photographs of Police targets involved in organised crime such as Automated Teller Machine (ATM) scams. Customs investigators also manually compare CCTV coverage of arriving and departing passengers with photographs of Customs targets taken during controlled deliveries of illegal drugs and precursor substances ("controlled deliveries" are where a consignment of, for example, illegal drugs is detected and allowed to go ahead under their control and surveillance in order to obtain evidence against the organisers).

Biometric technology could convert photographs of unidentified law enforcement and security targets into biometric information. Customs could then match this information in real-time against CCTV coverage of departing and arriving passengers. This would allow us to identify unidentified individuals of interest to Police, terrorist suspects, transnational criminals, and people who feature in surveillance from controlled deliveries of prohibited goods.

Other agencies also provide Customs with the names of particular people of interest – for example, people who are not permitted to leave New Zealand. If these people travel using other unknown aliases, then without biometric information Customs would be less effective in preventing them from leaving.

Customs' processes for protecting biometric information

We recognise that there are concerns and sensitivities around the collection and use of biometric information.

We currently protect biometric information in the same way as all information held by Customs: our servers are built to Government Restricted level and, for certain levels of information, access is restricted to only designated staff.

In addition, we secure biometric information both physically (through locks and surveillance) and electronically. No biometric information remains stored at SmartGate processing points. Live images are not directly accessible to other agencies.

Customs carries out frequent risk and security audits of SmartGate, and SmartGate information is protected by these specific security measures:

- the system generates automatic and regular reports for the appropriate managers, to prompt reviews of who has permission to access the SmartGate computer system
- when a staff member leaves Customs their access permission is cancelled
- access to the SmartGate computer system is audited every six months.

The confidentiality of biometric information is also protected by these measures:

- SmartGate uses local matching (that is, the person presenting the passport is matched against the biometric information in the passport's electronic chip) rather than remote matching to central biometric databases, which are potentially more vulnerable to abuses of privacy
- the Office of the Privacy Commissioner assessed and approved the Privacy Impact Assessments that Customs carried out on SmartGate before the system was used. Government agencies are required to carry out these assessments, which are a risk identification and management tool, whenever a new or amended initiative involves personal information.

Our preferred solution

Providing for Customs' use of biometrics in the Customs and Excise Act

We think it is important that we are up-front and open about our use of biometric information as a particular class of personal information. We also want to clarify how we are able to use biometric information when acting on behalf of other government agencies who are not present at the border. We think that having explicit authority for Customs to use biometric information for our own and for general law enforcement and security purposes would increase transparency. It would allow us to incorporate biometric information into our wider information-management framework. We would then be able to make the best use of this information as it becomes available, and also adapt to potential future uses, in our management of the border.

We also believe that providing for Customs' handling of biometric information in the Customs and Excise Act would clarify that we can then access and share this information for law enforcement purposes where this is authorised under our information sharing provisions and arrangements.

To avoid any confusion or uncertainty, we think Customs' legislation should not duplicate any powers that Customs already has under the Immigration Act 2009.

We consider that any provision dealing with the storage of biometric information should be aligned with the wider approach adopted for handling personal information in the Act. We note that our key international enforcement partner, Australia, stores biometric information for up to seven years so that it can be accessed for investigations and law enforcement purposes.

Other solutions we are considering

Status quo

Around the world, travel documents and border systems are becoming increasingly sophisticated, and Customs needs to be able to adapt to these changes. The status quo would leave Customs' ability to handle biometric information continuing to be governed by a combination of the Customs and Excise Act (for SmartGate), the Privacy Act, the Immigration Act, and other legislation.

We would also be limited in exploring future and emerging opportunities for the use of biometric information to enhance border security.

Who would be affected by change

International arriving and departing travellers already submit photographs (one form of biometric information) to Customs, whether this is by using SmartGate, or by passport-reading devices used by Customs officers. Customs also monitors CCTV feeds in the arrivals and departures areas at international airports. These are not currently biometric, but in future they could be capable of scanning faces to match them against images of people of interest.

Travellers would therefore not notice any significant change to current traveller processing. Any change to biometrics other than photographs would be subject to a Privacy Impact Assessment. The changes we propose would only be to clarify the purposes for which biometric information collected by Customs can be used and shared for Customs and law enforcement purposes.

BIOMETRICS: WHAT DO YOU THINK?

Q 29 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.

Q 30 If you do agree with that proposal, do you have a view on how long biometric information should be stored so that it can be used and shared for law enforcement purposes? Please give your reasons.

Q 31 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?

Virtual and digital goods

In this section, we look at the role of Customs in managing virtual and digital goods at the border as part of enforcing controls over restricted or prohibited imports. This section does not examine revenue or taxation issues relating to virtual or digital goods.

For more information on Customs' ability to examine and access a person's electronic devices (such as laptop computers and smartphones), see page 131 in the "Powers" chapter.

Throughout this section we will refer to virtual and digital goods as "digital files".

Terms used in this chapter

Virtual and digital goods: Also known as "digital files", these can include, for example, computer code, software, e-books, data files and video files.

The widespread use of digital technologies means that there are now numerous means by which digital files can be transferred across borders. They can be transmitted over the internet, or carried on laptops, smartphones and other devices. The instantaneous transfer of files challenges the traditional notions of border control.

Digital files are largely used by people for legitimate purposes, but there are situations where they are used to evade border controls.

Restricted items that would once have crossed the border in a physical form, such as a book, can now be carried in digital form. Sophisticated encryption of files means that it can be harder for Customs to detect illegal activity.

Customs' interest in relation to digital files is in the following enforcement areas:

- intercepting prohibited or restricted items
- identifying infringements of intellectual property rights.

> "Worldwide consumer spending on digital movies, games, and apps grew 30 percent from 2012 to 2013"

Customs will continue to intercept digital files at the border

In this review, we are not proposing to expand Customs' role in relation to digital files into areas such as actively monitoring cross-border internet traffic. We will continue our role of intercepting digital files that have content subject to an import or export restriction and that are transported across the border on a physical device, such as a laptop or portable hard drive.

As appropriate, Customs will also continue to investigate cases of import or export offences that are referred to us by a domestic agency, such as the Department of Internal Affairs, or by an overseas enforcement agency. These investigations could include exercising search warrants and following up on border interceptions of digital files on physical devices. Currently the most common types of prohibited digital files that we intercept and investigate are those containing objectionable material.

Other agencies have a lead role in relation to digital files

Agencies other than Customs have the main responsibility and capability for identifying and investigating offences relating to digital files. For example, the Office of Film and Literature Classification (OFLC) is responsible for classifying publications (including digital file formats) as objectionable material.

However, Customs' unique role of intercepting prohibited material when it is physically carried across the border means that we work alongside these other government agencies – for example, by submitting intercepted digital material to the OFLC for classification if we believe it may be objectionable.

Virtual and digital goods: The law as it stands

The Customs and Excise Act was developed largely before the emergence and expansion of the digital world. The Act's focus has been mainly on traditional travel, trade and commerce.

The Act defines "goods" as "moveable personal property". Some digital files do not meet this definition, and this means parts of the Act relating to importing and exporting goods do not apply to these digital files.

Our Act does enable us to enforce the law in relation to the following prohibited goods when they are in a digital format:

- objectionable material and images – "objectionable" has a very broad definition under the Films, Videos, and Publications Classification Act 1993, and can capture material ranging from violent or degrading sexual images to material that encourages criminal acts or terrorism
- designs for weapons or for other items of potential military use
- designs and blueprints for making nuclear, biological, chemical or radiological weapons.

If the Office of Film and Literature Classification classifies a publication as objectionable, then Customs has powers to investigate and to intercept imports and exports of these publications, including in digital formats.

Virtual and digital goods: Key issues and opportunities

We believe that our legislation needs to be both clearer and more flexible in defining the types of digital files that Customs can intercept. We want to ensure that our legislation can meet the current and future challenges of rapid digitalisation, and can complement any domestic controls that may apply, so that, for example, a restriction on possessing a particular digital file within New Zealand can be supported by restrictions on importing and exporting.

One particular area for attention is where imported digital files may fall outside the definition of "publication" in the Films, Videos, and Publications Classification Act and therefore outside Customs' current enforcement powers. Examples could include computer instructions for producing goods through 3D printing,[7] and computer malware.

Example of a gap in the legislation

It is an offence to access a computer system without authorisation – for example to introduce malware, such as a computer virus. However, malware brought across the border on an electronic device such as a laptop does not fall within the definition of "goods" in the Customs and Excise Act.

We expect that as technology advances, there will be new opportunities for importing prohibited goods through digital means. For example, several digital files may be imported that, when combined, would result in a prohibited item.

Solutions we are considering

We are considering the three options discussed below. We believe change is needed to keep up with changes in technology, but we do not have a view as to which of the two options for change would be best.

Status quo: Make no legislative changes

Under this option, there would be no change to Customs' responsibilities for policing certain types of digital files that constitute objectionable material, or that have a military/weapons design use or a prohibited "strategic" weapons use (designs for making nuclear, biological, chemical or radiological weapons).

We believe this option would prove increasingly impractical over time and that Customs would be unable to quickly adapt to new challenges presented by digital material.

[7] 3D printing is a process of making a solid three-dimensional object by a printer driven by instructions contained in a data file.

Prescribe which digital files are covered by the Act through Regulations

Under this option, a change to the definition of "goods" in the Customs and Excise Act would add the words "certain types of electronic goods". "Certain types of electronic goods" would then need to be defined or specified further, probably through Regulations made under the new Act. This could be done quickly as government policy changes in response to changes in technology.

This option would allow Customs to intercept, seize and investigate specific types of digital files that do not fall under the definition of "publication" in the Films, Videos, and Publications Classification Act, or that are not electronic publications classified as prohibited exports by Order in Council. Under this "opt in" approach, the list of types of digital files could be updated as new threats emerge. This would enable existing powers over the current range of digital files to be applied also to other specified digital files through a simple and transparent process.

Expand the definition of "goods" to cover all digital files unless specifically excluded

This option would give Customs the flexibility to control other types of digital files as new technologies emerge, and as concerns arise about harm to the community or to national security that are comparable to concerns for those digital files already covered in the legislation currently. This option would potentially bring all digital files within the ambit of Customs' legislation.

Like the previous option, this option would expand the definition of "goods" in the Customs and Excise Act by adding "certain types of electronic goods" to the definition.

This option would also expand the current provisions relating to importing and exporting goods to cover other types of digital files in the interests of public safety and national security, in addition to the specific digital files already covered in the Act.

The option differs from the second option presented above in that digital files would automatically come under the potential control of Customs. It would require amending the Act to **remove** any specified type of digital goods from Customs' control, whereas under the second option the Government would make a policy decision each time to place a digital file format or content under Customs' control through (most likely) Regulations.

Penalties for importing or exporting any new prohibited digital files would be in line with penalties for existing prohibited digital files.

Who would be affected by change

People importing or exporting digital files may be affected by the two change options we have put forward. Customs recognises that we will need to balance the rights of individuals with the need to protect the community and national security.

VIRTUAL AND DIGITAL GOODS: WHAT DO YOU THINK?

Q 32 Would you be affected by legislative change to Customs' powers in relation to digital files? If so, how?

Q 33 What do you think is the best option to address the gaps that have been identified? What are your reasons?

Q 34 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?

Business records

The Customs and Excise Act currently requires traders to keep their business records in New Zealand. This is to ensure that Customs has access to the records we need to be able to carry out audits under our revenue assurance obligations.

If there were no restrictions on where businesses records are kept, it is likely that Customs would not be able to give the same level of assurance to the Government and the public that the right amount of revenue is being collected and from the right businesses.

This requirement is, however, becoming increasingly impractical for businesses wanting to take advantage of cloud-based storage for their digital information. This is because cloud-based computing is usually located offshore.

By contrast, taxpayers can apply to Inland Revenue to store their tax records offshore, and this can include cloud storage.

Our preferred solution

Allow businesses to store business records offshore with Custom's prior approval

Our preferred option would allow businesses, and others such as a data storage provider on a business's behalf, to store their records offshore if they have Customs' prior approval. This would allow trusted businesses to take advantage of the opportunities offered by cloud storage and other evolving technologies.

This option would also align the Customs and Excise Act with the Tax Administration Act and allow Customs and Inland Revenue to jointly provide a better customer experience for businesses trading in New Zealand.

If we had concerns about the reliability of a particular business Customs could require it to keep its records in New Zealand, where we would have guaranteed access to them. As with the current Act, a penalty would apply if that business did not comply, and permission for offshore storage could also be revoked if Customs has evidence that the particular business is not complying with requirements.

We would develop criteria to be used to determine whether a business is eligible to store their records offshore. These criteria would be transparent, and they would be aligned to other government agencies' requirements to ensure that businesses are not having to meet very different requirements for different agencies. While Customs would assess each request for approval against those criteria, we would also take into account the particular circumstances of each individual case.

Examples of criteria that Customs might use in permitting a business to store records offshore

- the form and manner in which the information will be stored
- how accessible the information will be
- whether the business has breached any previous obligations for record-keeping or for providing Customs or other government agencies with access to those records.

Other solutions we are considering

Allow all businesses to store their records offshore

This option would allow all business to store their business records offshore if they decided to. This would enable businesses to take advantage of the opportunities provided by cloud storage and other technologies.

However, this may present a risk that Customs would be unable to verify business records to safeguard Crown revenue. If records are stored offshore they are effectively outside the jurisdictional reach of the Customs and Excise Act. This means Customs would not provide the same level of assurance to the Government and the public that the right revenue is being collected and from the right businesses.

Status quo

Retaining the status quo would require all businesses to continue storing their business records in New Zealand. This would allow Customs to maintain confidence that at all times we have access to the records we need, but it would constrain businesses from taking advantage of technological advances.

The status quo is also inconsistent with other government agencies' requirements, particularly Inland Revenue.

Who would be affected by change

There are likely to be lower compliance costs for those businesses that are granted approval to store their records offshore, as they would be able to use more cost-effective storage methods. All businesses that are required by us to store records could be affected by changes to the current storage requirements.

BUSINESS RECORDS: WHAT DO YOU THINK?

Q 35 How would maintaining the status quo (that is, requiring business records to be kept in New Zealand) affect you or your business? If possible, please provide examples that show the scale of any obstacles or issues that this would present for you or your business.

Q 36 If you were to store your business records offshore, what benefits would this have for your business?

Q 37 Which option do you prefer? Please give your reasons.

Q 38 Are there other parts of the Customs and Excise Act that you think need to be updated because they do not support the use of digital technology or other technological changes in your operating environment?