# A LEGAL FRAMEWORK FOR SHARING CUSTOMS INTELLIGENCE THROUGH THE SINGLE WINDOW SYSTEM

BY

BRUCE WAI-MING THOMAS

A thesis
submitted to the Victoria University of Wellington
in fulfilment of the requirements for the degree of
Doctor of Philosophy

VICTORIA UNIVERSITY OF WELLINGTON

2018

## *Acknowledgements*

I would like to thank everyone who assisted me in the preparation of this thesis. My wonderful wife Stacey, and my two sons, Sacha and Elliot, have been very patient and tolerant of the time that I have spent working at this, rather than with them.

I am indebted to the men and women of the New Zealand Customs Service and the other government agencies that participated in, and supported, this research. The time and input that they offered was invaluable.

I will be eternally grateful to the superhero neurosurgeons and the team at Wellington Hospital: to Ales Aliashkevich, who used his remarkable skill to remove my brain tumour and save my life; and to Andrew Parker, for his expert aftercare.

The faculty of the Law School has been very understanding and supportive throughout the extraordinarily long time - ten years - that I have taken to complete this research. I am very thankful for the care, advice and encouragement provided by the faculty, especially the Postgraduate administrator, Jonathan Dempsey, and my secondary supervisor, Prof Tony Smith.

Most importantly, I will always be grateful to my primary supervisor, Prof Tony Angelo. He spent countless hours providing me with gentle encouragement, friendly guidance and expert advice. I am humbled by the time and effort that he has invested in me. I would not have completed this thesis, but for his enduring support. I am very proud to have been his student.

# Abstract

Some customs agencies are implementing electronic single window systems. These single window systems enable an importer or exporter to digitally transmit their transaction information to the customs administration. The single window system shares relevant information with other government agencies involved in the import or export process. It relieves the importer or exporter of the need to lodge transaction information separately with each government agency.

An international single window system is the interconnection of two or more national single window systems. It enables the exporter's transaction information to be re-used in import processing, thereby reducing the amount of information required from importers.

For states that already have customs intelligence-sharing agreements, a single window system could be used to exchange intelligence information about the import and export transactions processed by the system.

Intelligence-sharing agreements can and should include transparent protection for human rights. The human rights relevant to this legal framework are access to justice, freedom from arbitrary search and seizure, freedom from torture and the right to privacy. The right to privacy is the human right most affected by intelligence-sharing.

This thesis proposes a legal framework to enable intelligence to be shared through a single window system with transparent terms for managing human rights. This thesis suggests that public confidence would be improved by showing how privacy and other human rights are treated in the rules for customs intelligence-sharing using the system proposed here.

# Contents

ACRONYMS....11
GLOSSARY....15
CHAPTER ONE – INTRODUCTION....19
I The Thesis....19
A The Setting....20
B Public Support....23
II Method....24
A Introduction....24
B Stage I. Establishing the Criteria for the Legal Framework....24
C Stage II. Evaluating the Existing Landscape....25
D Stage III. Developing a Legal Framework....26
E Stage IV. Interviews....26
F Stage V: Conclusion....28
III Scope....28
IV The Single Window....30
A Why Single Window Systems are Needed....30
B How the Single Window Works....32
C Extent of use....33
D State Implementations....35
E How the Single Window System might be Used....38
V The Contribution to Knowledge....40
A Privacy....40
B Transparency....41
VI Potential Benefits....41
VII Chapter Summary....43
CHAPTER TWO – INFORMATION, SECRECY AND PUBLIC CONFIDENCE....45
I The Risk-Assessment Process....46
II The Information Needed for Trade Risk-Management....49
III The National Security Role of Customs....54
IV State National Security and Law Enforcement Objectives....57
V The Need for Secrecy....61
VI Transparency and Public Confidence....65
VII Factors Influencing Intelligence Cooperation....68
VIII Chapter Summary....73
CHAPTER THREE – AREAS WHERE TRANSPARENCY CAN AND SHOULD EXIST....75
I The Consequence of Human Rights....76
II The Right of Access to Justice....79
III Protection from Arbitrary Search and Seizure....83
IV Freedom from Torture....86
V Privacy, Law Enforcement and Security....91
VI Privacy and the Secrecy of Personal Information....95
A The Right to Privacy....95
B Activities that Harm Privacy....99
1 Information collection....100
2 Invasions....101
3 Information processing....101
4 Information dissemination....104
VII Chapter Summary....107
CHAPTER FOUR – ESTABLISHING A BENCHMARK FOR TRANSPARENT PRIVACY....109
I Privacy, Databases and Other Electronic Systems....109
II Changes since 11 September 2001....113

III The Snowden Leaks ... 117
IV The Tort of Privacy ... 119
V Privacy Legislation ... 127
A Privacy Principles: Basic Principles of National Application ... 128
1 Collection Limitation ... 128
2 Data Quality ... 128
3 Purpose Specification ... 128
4 Use Limitation ... 128
5 Security Safeguards ... 128
6 Openness ... 128
7 Individual Participation ... 128
8 Accountability ... 129
B Privacy Principles: Basic Principles of International Application ... 129
1 A data controller is accountable ... 129
2 Limit restrictions to transborder flows of personal data ... 129
3 Restrictions are proportionate to risk ... 129
C Domestic Implementation of the Privacy Principles ... 130
VI Privacy Principles Applied to the Legal Framework ... 134
A Collection Limitation ... 135
B Data Quality ... 135
C Purpose Specification ... 136
D Use Limitation ... 137
E Security Safeguards ... 137
F Openness ... 137
G Individual Participation ... 137
H Accountability ... 138
I Absence of a Centralised Database ... 139
J Basic Principles of International Application ... 140
1 A data controller is accountable ... 140
2 Limit restrictions to transborder flows of personal data ... 140
3 Restrictions are proportionate to risk ... 140
VII Privacy Principles, Solove's Taxonomy and the Intelligence Lifecycle ... 140
VIII Chapter Summary ... 141

CHAPTER FIVE – HOW OTHER ARRANGEMENTS COMPARE ... 143
I The Measures of Successful Legal Framework ... 144
II Bilateral Agreements ... 146
A New Zealand – United Kingdom 1996 ... 148
B WCO Model Agreement 2004 ... 150
C New Zealand – South Korea Free Trade Agreement 2015 ... 153
D Summary of the Bilateral Agreements ... 154
III Existing and Past Multilateral Agreements ... 157
A The Nairobi Convention 1977 ... 161
B Johannesburg Convention 2003 ... 163
C SIRENE System 2013 ... 164
D Summary of the Multilateral Agreements ... 168
IV Other Information-sharing Agreements ... 171
A Five Eyes 1947 ... 173
B The INTERPOL System 1956 ... 178
C PNRGOV System 2013 ... 183
D Summary of Multilateral Agreements ... 187
V Chapter Summary ... 189

CHAPTER SIX – OUTLINE OF THE PROPOSED LEGAL FRAMEWORK ... 191
I The Purpose of the Legal Framework ... 191
II The Intelligence-sharing Process ... 192
A Reservations and Non-Compliance ... 193
B Avoiding Manipulation ... 194

C Lawfully Obtained Information ... 194
D Available Process to Challenge the Accuracy of Information ... 194
E Maintaining Confidentiality ... 194
F Transshipments ... 196
G Correcting and Updating Information ... 196
H Notice to Subjects of Information ... 198
I The Data Controller ... 198
J Damages and Penalties ... 200
K Administration ... 201
III Chapter Summary ... 202

CHAPTER SEVEN – EVALUATION OF THE PROPOSED LEGAL FRAMEWORK ... 203
I The Interviews ... 203
II Enabling Trust between States and State Autonomy ... 205
A Information Access and Disclosure Control ... 206
B Audit, Review or Self-Reporting of Compliance ... 206
C Information Retention and Destruction Controls ... 206
D Voluntary, Not Compulsory, Information-sharing ... 207
III Transparency for the Privacy Principles ... 208
A Collection Limitation ... 209
B Data Quality ... 209
C Purpose Specification ... 209
D Use Limitation ... 210
E Security Safeguards ... 210
F Openness ... 210
G Individual Participation ... 211
H Accountability ... 212
IV Transparent Protection for Other Human Rights ... 212
V Enabling Intelligence-sharing for Customs Risk-management ... 213
A Terms that Enable Intelligence-sharing ... 213
B Common Standards/Format for Information Exchange ... 214
C Terms that Enable Real-Time Electronic Exchange ... 214
VI Other Implementation Options ... 214
VII Chapter Summary ... 217

CHAPTER EIGHT – CONCLUSION ... 219

APPENDIX ONE – INTERVIEWS ... 223
I Consent Form ... 224
II Interview: Usefulness to Intelligence Users ... 225
III Interview: Privacy ... 227

APPENDIX TWO – PROPOSED CONVENTION ... 231

APPENDIX THREE – MODEL LAW ... 247

BIBLIOGRAPHY ... 263

# Index of Figures

Figure 1. Intelligence lifecycle ..... 29
Figure 2. Border transactions without a single window ..... 33
Figure 3. Border transactions in a single window environment ..... 34
Figure 4. The international single window concept ..... 34
Figure 5. ASEAN single window Pilot Project 2011-2013 ..... 35
Figure 6. Border risk-management ..... 47
Figure 7. Some entities involved in an import/export transaction ..... 51
Figure 8. Solove's taxonomy of privacy ..... 99
Figure 9. Solove's taxonomy within the intelligence lifecycle ..... 100
Figure 10. The Privacy Principles and thesis scope mapped to Solove's taxonomy of privacy ..... 141
Figure 11. Implementation of the measures in bilateral agreements ..... 157
Figure 12. Implementation of the measures in multilateral agreements ..... 171
Figure 13. Implementation of the measures in other models for information-sharing ..... 189
Figure 14. Comparison of all models to the measures established for the legal framework ..... 190
Figure 15. The proposed single window intelligence-sharing process ..... 192

# Index of Tables

Table 1. Interviews ..... 27
Table 2. Facilitators of, and barriers to, single window implementation ..... 36
Table 3. Application of OECD principles in a selection of states ..... 130
Table 4. Measures used to evaluate information-sharing agreements ..... 146
Table 5. Bilateral agreements assessed ..... 147
Table 6. Summary of bilateral agreement assessments ..... 156
Table 7. Multilateral agreements assessed ..... 158
Table 8. Summary of multilateral agreement assessments ..... 170
Table 9. Other information-sharing models assessed ..... 172
Table 10. Summary of other information-sharing model assessments ..... 188
Table 11. Summarised assessment of the proposed legal framework ..... 218

# Acronyms

**AEO** is an Authorised Economic Operator, which is a party involved in the international movement of goods that has been approved as complying with World Customs Organisation (WCO) supply chain security standards.

**API** means Advanced Passenger Information, which is an extract of data from the database of an air travel operator which is combined with government immigration information to confirm the validity of a passenger's visa and other travel documentation at check-in.

**APEC** is the organisation for Asia-Pacific Economic Cooperation.

**ASEAN** is the Association of South East Asian Nations.

**CARIFORUM** is the Forum of Caribbean States.

**CIA** is the United States Central Intelligence Agency.

**CERT** means Cyber Emergency Response Team.

**CITES** is both the Convention on International Trade in Endangered Species of Wild Flora and Fauna and the name of the organisation that administers the Convention.

**CPO** is a Chief Privacy Officer.

**C-TPAT** is the Customs-Trade Partnership Against Terrorism, a voluntary supply-chain security program operated by United States Customs and Border Protection which aims to protect the supply chains of private companies against terrorism.

**ECHR** is the European Convention on Human Rights.

**EDIFACT** is the Electronic Data Interchange for Administration Commerce and Transport standard for information processing.

**ETA** is Euskadi Ta Askatasuna, a Basque nationalist and separatist organisation.

**EU** is the European Union.

**EU-LISA** is the EU Agency for the operational management of large-scale IT systems.

**EuroPol** is the European Police system for European Union members to enable mutual assistance between their police authorities.

**FATCA** is the Foreign Account Tax Compliance Act system established by the United States to target tax non-compliance by United States taxpayers with foreign accounts.

**FATF** is the Financial Action Task Force.

**FBI** is the United States Federal Bureau of Investigation.

**FLN** is the National Liberation Front of Algeria.

**FTA** is a Free Trade Agreement.

**GCHQ** is the United Kingdom Government Communications Headquarters, a government agency responsible for collecting electronic computer and signals intelligence.

**GCSB** is the New Zealand Government Communications Security Bureau, a government agency responsible for collecting electronic computer and signals intelligence.

**GLIC** is the Global Liberty Internet Campaign.

**IATA** is the International Air Transport Association.

**ICAO** is the International Civil Aviation Organisation.

**ICCPR** is the International Covenant on Civil and Political Rights.

**ICPC** is the International Criminal Police Commission, the predecessor to INTERPOL.

**ICS** is the transaction-processing system of the Australian Customs and Border Protection Service.

**INTERPOL** is the network of police forces from 190 countries that work together to solve crimes that cross borders.

**NSA** is the National Security Agency of the United States.

**NZSIS** is the New Zealand Security Intelligence Service, an intelligence agency responsible for protecting New Zealand from threats of espionage, sabotage and subversion.

**OECD** is the Organisation for Economic Co-operation and Development.

**OIA** is the New Zealand Official Information Act 1982.

**PNR** means Passenger Name Record, which is a record in the database of an international air travel operator.

**PNRGOV** is the PNR Government initiative of the WCO, IATA and ICAO to ensure passengers have valid travel documentation and to assist states to risk-assess passengers and their baggage

**SCCP** is the APEC Sub-Committee on Customs Procedures.

**SES** is the Secure Export Scheme, an Authorised Economic Operator system that certifies supply chains between New Zealand and the United States.

**SIRENE** is the Supplementary Information Request at the National Entries, the European Union IT system for customs enforcement cooperation.

**SIS II** is the second-generation Schengen Information System.

**TPP** is the Trans Pacific Partnership.

**UCR** is the World Customs Organisation Unique Consignment Reference.

**UDHR** is the Universal Declaration of Human Rights.

**UK** is the United Kingdom.

**UN** is the United Nations.

**UN/CEFACT** is the United Nations Centre for Trade Facilitation and Electronic Business.

**UNCITRAL** is the United Nation's Commission on International Trade Law.

**UNECE** is the United Nations Economic Commission for Europe.

**UNTDED** is the United Nations Trade Data Elements Directory standard for information processing.

**US** or **USA** is the United States of America.

**WCO** is the World Customs Organisation.

**WCO Data Model** means the information framework first published by the World Customs Organisation as the WCO Customs Data Model in January 2002 and updated from time to time to standardise and simplify Customs data requirements.

**WMD** is Weapons of Mass Destruction.

**WTO** is the World Trade Organisation.

**XKEYSCORE**, is allegedly a NSA-led mass data collection system.

**XML** is Extensible Mark-up Language, a standard for information processing.

# Glossary

**9/11 terrorist attacks** means the Al Qaeda terrorist attacks in the United States on 11 September 2001.

**Big Data** means data held in such large amounts that it can be difficult to process, but which can, through the linking of metadata, be used to build a profile of an individual or track their activities (an indirect means of surveillance).

**Controls** are rules and methods that help to ensure the accuracy and validity of information or compliance with the objectives of the legal framework.

**Craft** means the vehicles or sea-going vessels that are used to transport goods.

**Customs** and **customs administration** mean a state's agency(s), and potentially its private contractors, which enforce the state's law regarding the flow of goods and other material through its borders. For example, in the United Kingdom the customs function is part of the agency that is responsible for revenue collection (taxation).[1]

**Customs law** means any legal and administrative provisions applicable or enforceable by the customs administration in connection with the importation, exportation, transshipment, transit, storage and movement of goods, including legal and administrative provisions relating to measures of prohibition, restriction, and control of, and in connection with combating money laundering.

**Customs offence** means any violation or attempted violation of customs law.

**Entity** means any party to a trade transaction, or any location, means of transport, business or any other physical thing or abstract concept that can be related directly or indirectly to the trade transaction and for which there is information useful to the risk-management of the trade transaction.

**Five-Eyes** is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States.

**Information** means any data in any format that may be obtained from the public domain, or directly from the parties to the trade transaction, or from any other sources to which the state party has access.

**Intelligence** means verifiable or unverifiable information related to the trade transaction or an entity which is considered relevant to risk-management and of which the existence, possession or use of such information is deemed a secret by the providing state party. Intelligence information can be received from a variety of sources, including from the

[1] Her Majesty's Revenue and Customs Service "About Us" (2008) Her Majesty's Revenue and Customs Service <customs.hmrc.gov.uk>.

subject of the risk analysis. Intelligence can be received from open or public domain sources such as the Internet or public registers. It can also be received from closed or restricted sources, including domestic and foreign government agencies. Intelligence information can relate to any of the entities involved in the risk-assessed transaction. For example, intelligence can relate to the risk of trading with a particular region, state, commercial or residential address, organisation or person. It can also relate to the risk of trading particular types of goods or transacting through intermediaries such as a specific carrier or agent. Often, an intelligence holding must remain secret from the subject to protect the integrity and effectiveness of threat targeting and investigation techniques.

**OECD Privacy Framework** is a framework of privacy principles and guidelines published by the Organisation for Economic Cooperation and Development.

**Official** means any customs officer or other government agent designated by a state party to apply customs law.

**Party to the trade transaction** means the exporter, the importer, or any other person or organisation involved in the processing or transit of the trade transaction.

**Person** means both natural and artificial legal persons.

**Personal information**

(a) for natural persons, means information or an opinion, whether true or not, about or from an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion;[2]

(b) for artificial legal persons, means information that can reasonably be considered prejudicial to the commercial position of the person who is the subject of the information;[3]

**Privacy Principles** means the privacy principles of the OECD Privacy Framework.

**Provided information** means information shared between customs administrations.

**Providing state party** means the state party whose customs administration is requested to provide information;

**Providing administration** means the customs administration from which information is requested.

**Real-time** and **in real time** refers to the processing of information quickly so that decisions can be made and actions can be taken without delay, usually through the use of electronic and computerised system.

[2] Adapted from the Privacy Act 1988 (Australia), s 6.

[3] Adapted from Official Information Act 1982 (New Zealand)(OIA), s 9(2)(b).

**Requesting administration** means the customs administration which requests information.

**Requesting state party** means the state party whose customs administration requests information.

**Reservation** has the same meaning as in the Vienna Convention on the Law of Treaties (1969) 1155 UNTS 331.

**Risk-assessment** and **risk-management** mean the assessment of all available information pertinent to a border transaction to enable a decision on whether customs intervention in that transaction is appropriate and the actions taken in making that intervention.

**Single window** means an implementation of the UN/CEFACT initiative for the facilitation of trade transactions.[4] The term single window is generally used here in the context of sharing information internationally between single window systems.

**Trade transaction** means the information and processes involved in the cross-border movement of goods from the point of export to the point of import.

**Transparent** means the terms are accessible and understandable so that people can trust that they are fair and honest.[5]

**Transshipment** means the transfer of goods from one carrier or vessel to another at an intermediate destination while those goods are in transit from the point of export to the point of import.

**Unauthorised disclosure** means the release of any provided information to any other state party, customs administration, organisation or person where that information is not available in the public domain and where the disclosure has not been explicitly permitted by the providing administration.

[4] *Recommendation No. 33: Recommendation and Guidelines on establishing a Single Window* ECE/TRADE/352 (2005). See also WCO "WCO Encourages One-Stop Service at Borders" (9 August 2005) World Customs Organisation <www.wcoomd.org>.

[5] Adapted from Cambridge University Press *Cambridge Business English Dictionary* (Cambridge University Press, Cambridge UK, 2011).

# Chapter One – Introduction

## *I The Thesis*

Customs administrations use single window systems to receive trade transaction information electronically from importers and exporters so that it may be processed.[6] Customs administrations also use single window systems to transmit responses back to the importers and exporters.[7] Customs administrations lead the implementation of single window systems because the single window concept is an initiative of the World Customs Organisation (WCO).[8]

Customs administrations use intelligence in separate processes to identify high risk transactions for intervention.[9] The intelligence can be shared with other customs administrations through manual practices.[10] The agreements that enable customs intelligence-sharing are deficient in their treatment of human rights, often because governments exempt security and law enforcement activity from privacy compliance.[11] As a result, members of the public do not know how its information is being managed in these settings. This lack of transparency affects public confidence in the intelligence-sharing process. The lack of clarity is also a challenge for governments wanting to create new intelligence-sharing partnerships.

The thesis is that, with an appropriate legal framework, a single window system could be used to automate intelligence exchanges with transparent terms for managing human rights. This thesis suggests that public confidence would be improved by showing how privacy and other human rights are treated in the rules for customs intelligence-sharing processes. It should be noted, however, that this thesis does not include an empirical study to gauge the effect of the proposed legal framework on public confidence.

---

[6] For examples see European Commission "Electronic Customs Multi-Annual Strategic Plan" (21 November 2014) European Commission <ec.europa.eu> and Malta Customs "Customs Electronic System (CES)" (2103) Malta Customs <customs.govt.mt>.

[7] Single window systems are discussed further in Part IV of this Chapter.

[8] WCO, above n 4.

[9] Emilia Iordache and Alina Vasilica Voiculet "Customs Risk Management in the European Union" (2007) 10(25) Romanian Economic Journal 55, at 63. This is discussed further in Chapter Two.

[10] This is also discussed in Chapter Two. Analysis in Chapter Five shows that existing international agreements do not generally enable customs intelligence to be shared automatically, using an electronic system.

[11] The analysis in Chapter Five shows the extent to which the existing international agreements typically stipulate terms for managing privacy and other human rights.

The principles of the OECD Privacy Framework, which have been endorsed by the 25 member-states of the OCED and the 27 member-states of the EU, are adopted as the most widely accepted statement of public expectations for privacy. A normative analysis of the extent to which the OECD privacy principles capture public expectations of privacy is not offered here.

The logic of the thesis is that -

1. there is no law enabling customs to share intelligence electronically and in real-time for risk management purposes; and
2. the privacy principles of the OECD Privacy Framework are the most widely accepted expression of public expectations for the treatment of privacy; and
3. with some exceptions, the principles of the OECD Privacy Framework can be imposed as controls on a practical intelligence-sharing arrangement; and
4. making those controls transparent should improve public confidence; so
5. a legal framework that allows customs administrations to share intelligence through the transactional single window system, and at the same time show how privacy and other human rights are treated, should improve public confidence.[12]

This work addresses the question: "What would a legal framework that enables customs administrations to share intelligence through a single window system look like?". The product is a legal framework comprising an international Convention and a Model Law for domestic implementation.

The circumstances that suggest the promulgation of the legal framework are that:

1. single window systems already exist for governments to automate aspects of trade transaction-processing; and
2. customs administrations use manual processes to share intelligence.

### *A The Setting*

Single window systems are used by customs administrations in many states to enable traders to lodge import and export information with government agencies. With a single window system, the traders need to submit information only once. The responses from each government agency are aggregated into a single response for the trader.

Single window systems can remove the need for paper-based transactions and the need for separate lodgements with individual government agencies. In some states, 30 or more

[12] OECD "The OECD Privacy Framework" (2013) OECD <www.oecd.org>.

government agencies are involved in processing the transaction.[13] Consequently, a single window system can remove the need for manual processing. The benefits include transaction-processing at lower cost for traders and governments.

Some regions have implemented international single windows.[14] States in those regions connect their national single windows together so that the export lodgement can be shared with the importing state. The importing state government can process the transaction with this information, so little or no further information is needed from the importer.

Much of the intelligence used by customs administrations is shared through manual practices. However, non-intelligence information is increasingly shared through automated, electronic exchanges.[15] Customs administrations receive intelligence from many sources to help them to risk-assess trade.[16] Transactions and all the parties involved in the transaction are risk-assessed. Low risk transactions are cleared to proceed. High risk transactions are singled out for intervention.[17] For example, to determine the risk level of a shipment from a Chinese exporter to a New Zealand importer, a customs administration might want to know –

- Does the importer or exporter, or the people they associate with, have a criminal background or a history of making false declarations? For example, there may be a record of false declarations made by the person or other people at the same address, or there might be information that indicates the person is part of a criminal network.
- Do the goods make sense for the business they are in? For example, if the business sells furniture, an import of engine parts would be unexpected.
- Does the transaction fit the profile of their previous transactions?

[13] "WCO Research paper No. 17: A Survey of Single Window Implementation" (2011) World Customs Organisation <www.wcoomd.org>.

[14] Electronic Customs Multi-Annual Strategic Plan: 2008 Yearly Revision [2008] TAXUD/477/2004 - Rev 9 – EN; and JKT Tsen "Ten years of Single Window Implementation: Lessons Learned for the Future" (13 December 2011) United Nations Economic Commission for Europe <unece.org>.

[15] For example, see Michele Wilson "Community in the Abstract: A Political and Ethical Dilemma" in David Holmes (ed) *Virtual Politics: Identity and Community in Cyberspace* (Sage Publications, London, 1997) 145, at 5. See also Daniel J Solove "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53(6) Stan L Rev 1393, at 1401

[16] George A Rennie "HM Customs and Excise IT and Intelligence Applications in Cross Border Control" (1998) (January) European Police and Government Security Technology 8, at 8.

[17] European Commission Customs Policy Committee *A Guide to Risk Analysis and Customs Controls* (Office for Official Publications of the European Communities, Luxembourg, 1999), at 47. More detailed lists of risk indicators are restricted to WCO members but are referred to in the index of the WCO "WCO Customs Risk Management Compendium" (2015) World Customs Organisation <www.wcoomd.org>, at III.

- Is the transaction unusual when compared to other businesses of the same type?
- Are there risks that weapons or weapons parts are involved?
- Is the type of goods often counterfeited?
- Are there indications that the goods are not from China at all? Traders from other states may try to benefit from reduced tariffs in the Free Trade Agreement (FTA) between New Zealand and China.

If there are indicators that a transaction might be suspect, customs seeks intelligence to help it risk-assess the transaction.[18]

However, the manual intelligence-sharing process is very labour intensive. Phone calls are often made because they are faster than other methods for sharing intelligence with a low security rating.[19] Consequently, intelligence-sharing relies heavily on maintaining personal relationships. This is because it is not practical for customs staff members to know and be able to identify every staff member in foreign customs administrations that might seek intelligence information.

The analysis in Chapter Five shows that there are no existing international agreements that enable customs agencies to exchange intelligence electronically and in real-time through a system like the single window. Systems exist for sharing criminal information, such as INTERPOL, the cooperative network of police forces from 190 countries, and Europol, the European policing cooperation system. However, those arrangements are not suitable for sharing intelligence to risk-manage trade transactions.[20]

There is an electronic system in the European Union (EU) for sharing customs information, but that system is designed to direct customs agencies to stop and seize specific goods or make an arrest.[21] It is not designed to facilitate the risk-management of every transaction.

[18] For more information on the risk-assessment process used by New Zealand Customs, see Rebecca Foley and Bruce Northway "Managing Risk in Customs: Lessons from the New Zealand Customs Service" (2010) World Bank <openknowledge.worldbank.org>.

[19] Discussed in an interview with Interviewee One. See Chapter Seven.

[20] INTERPOL "Overview" (2015) INTERPOL <www.interpol.int> and Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53. The reasons why are these systems are unsuitable are discussed in Chapter Five.

[21] Decision 2007/533/JHA on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II) [2007] OJ L205/63.

With an appropriate legal framework, a single window system could be used to automate many of the manual intelligence exchanges that already take place between customs administrations.

There are many factors that influence the development of intelligence cooperation.[22] For this reason, the legal framework proposed here will not satisfy all the requirements for creating new intelligence cooperation arrangements. However, it does enable the automation of existing intelligence-sharing practices through a single window system.

Using a single window system to exchange intelligence about the trade transactions processed by the system will produce benefits.[23] Automated intelligence exchanges would remove manual effort and a reliance on personal relationships. With intelligence in a consistent electronic format, some risk-management tasks could also be automated. It would make the targeting of transactions for intervention faster and more consistent, which in turn would lead to faster clearances and lower costs for businesses and government.

### *B Public Support*

Sharing intelligence through the single window would need public support and the backing of customs administrations. Customs administrations need the system to be workable and effective. In relation to public support, much has been said in the media about public distrust of secret intelligence activities.[24] The analysis here shows that procedures for managing human rights and privacy are absent from the majority of the international agreements that enable customs administrations to share intelligence. As a result, the public has no knowledge of how their interests are managed. The lack of transparency affects public confidence in the intelligence-sharing process. It also creates a challenge for governments wanting to create new intelligence-sharing partnerships.[25]

To improve public confidence, the treatment for human rights should be apparent in a legal framework for intelligence-sharing through a single window system. The treatment of human rights can be evident, even though the intelligence that is shared must stay secret.

There are six Parts in the remainder of this chapter. Part II describes the method used to develop and test the proposed legal framework. Part III sets out the scope and limitations of the work. The single window system is described in Part IV, along with a discussion

[22] An outline of these factors is provided in Chapter Two.

[23] Sarah L Garcia "Multilateral Cooperation: A New Look at Information Sharing" (2005) The Inter-American Defense Board <library.jid.org>, at 10. The benefits are discussed further in Part VI of this Chapter.

[24] This is discussed in Chapter Two.

[25] This is discussed in Chapter Two.

of the benefits that might result from sharing intelligence through the single window. Part V shows how this work contributes to academic knowledge by offering a legal framework where no equivalent legal framework exists. Part VI lists the potential benefits that would result from using the legal framework. The Chapter is summarised in Part VII.

## *II Method*

The following method was used to develop the thesis in 3 distinct stages.

### *A Introduction*

In this Chapter, the thesis, method and scope are outlined. The single window system is described with a view to putting this research in context.

### *B Stage I. Establishing the Criteria for the Legal Framework*

The logic of this thesis is that there is no law enabling customs to share intelligence electronically and in real-time for risk management purposes. This stage establishes the criteria that would enable customs administrations to share intelligence through a single window system. It sets out the practical requirements of customs administrations, at a high level. It also discusses the reasons why the treatment of privacy and human rights is desirable in a security and law enforcement information-sharing arrangement such as the one proposed here. The discussion describes the background to the development of the legal framework, but it does not seek to solve every problem that is identified. It does not seek to prove the value of protecting human rights. The aim of the thesis is to produce a legal framework that supports a practical system for customs administrations to share intelligence in a way that might improve public confidence in such intelligence-sharing.

A literature review was undertaken to establish the intellectual context or purpose of customs intelligence-sharing and to discover the types of information that are shared. The analysis, in Chapter Two, identifies the essential operational requirements that customs administrations have for sharing intelligence through a single window system. The standards associated with single window systems are examined to identify whether they could be extended to enable intelligence-sharing through these systems. The Chapter also describes the need for secrecy in customs intelligence-sharing and provides some of the reasons why this secrecy can erode public confidence.

Chapter Three describes the human rights which, if prudently treated, should lead to improved public confidence in intelligence-sharing.[26] United Nations (UN) instruments

[26] The transactional trading data, as opposed to intelligence information, used by customs administrations typically does not contain personal information. Consequently, that data has little relevance to human rights issues. Transactional trade data involves information about the description and value of the goods, the commercial parties (businesses) involved, the source address, destination address and the method of shipment.

for human rights are accepted here as benchmarks for their treatment. The Chapter provides some examples of issues and commentary that have occurred in relation to the abuse of these rights, especially in law enforcement, security and intelligence contexts, both before and after these rights were set down by the UN. This Chapter proceeds on the basis that it makes no normative arguments regarding the expression or value of these human rights. However, it argues that, because the proposed legal framework involves the exchange of personal information, privacy is the human right most affected by customs intelligence-sharing. Other human rights are affected only indirectly. Issues encountered in other intelligence and policing cooperation arrangements and the relevance of those issues to the proposed legal framework are also identified and discussed in Chapter Three to provide context.

The privacy principles that should be transparently treated to improve public confidence are identified in Chapter Four. It is not the purpose of this Chapter to make normative statements about privacy nor does it develop and test a novel set of privacy principles. Instead, it embraces the Privacy Framework of the Organisation for Economic Cooperation and Development (OECD) as the most widely accepted public expression of privacy values.[27] The thesis proceeds on the assumption that the inclusion of these privacy principles in the proposed legal framework will be acceptable to the public. It makes the assumption that, because the principles of the OECD Privacy Framework are the most widely accepted privacy principles, the inclusion of these principles in the legal framework should improve public confidence in customs intelligence activities. It does not examine the extent to which public confidence would be improved. Public acceptance of the legal framework with the inclusion of these principles would be tested in other forums. In New Zealand this could include parliamentary debate, select committee processes and the courts.

### *C Stage II. Evaluating the Existing Landscape*

This stage supports the claim this thesis makes that there is currently no law that enables customs administrations to share intelligence electronically and in real-time for risk management purposes. It evaluates the existing landscape and determines the extent to which existing information-sharing agreements and models include terms that would be suitable for enabling customs to share intelligence through a single window system.

The customs, human rights and privacy criteria that are described in Chapters Two, Three and Four are summarised as a set of measures in Chapter Five. The set of measures is a benchmark for evaluating the proposed legal framework.

Thirty bilateral and multilateral agreements that enable customs administrations to share information are examined to find out whether any of these agreements contain all the

[27] OECD Privacy Framework, above n 12.

criteria that would be needed to implement intelligence-sharing through a single window system. These were all the agreements that were accessible for this analysis. They include Memoranda of Understanding between customs administrations that were not readily accessible to the public, but which were provided for the purposes of this study.

A small collection of these agreements is compared and discussed in Chapter Five to demonstrate the extent to which customs information-sharing agreements typically implement the measures established above for sharing intelligence through a single window system.

A small selection of other intelligence and information-sharing models is also examined to provide further insight into the degree that the measures established above are commonly applied, or absent, in other types of information-sharing agreements.

### *D Stage III. Developing a Legal Framework*

This stage supports the claim that a legal framework can allow customs administrations to share intelligence through the transactional single window system and at the same time show how privacy and other human rights are treated. It develops a new legal framework to permit the sharing of intelligence through a single window system. The new legal framework is evaluated against the same measures that were used to assess existing information-sharing agreements and models in Stage II.

Chapter Six discusses the proposed legal framework. It is comprised of a Convention and Model Law for domestic implementation. It was drafted to incorporate the essential criteria set out in Chapter Five. The full texts of the Convention and Model Law are included in Appendices I and II.

The proposed legal framework is evaluated in Chapter Seven against the measures and compared with the results of the evaluations undertaken in Chapter Five. This evaluation shows that the legal framework is a better model for sharing customs intelligence through the single window than the other models that were examined.

### *E Stage IV. Interviews*

Chapter Seven includes key points from interviews with ten New Zealand experts in security and law enforcement intelligence-sharing, customs issues and the management of intelligence-sharing relationships. Feedback was sought from these intelligence experts on whether the draft framework contained what they viewed to be the essential elements of a practical and effective framework for their needs. The draft Convention was provided to these people for reassurance that the proposed framework is practical and fit for purpose. The interviews provided assurance over the analysis and reasoning applied to the preparation of the legal framework. The interviews were not intended or used as an empirical research method to derive specific elements or evidence upon which the framework is based. Likewise, the purpose of the interviews was not to extract

cultural and socio-legal understanding of the trust and confidence issues in customs intelligence-sharing relationships. Nonetheless, interesting comment was offered and noted. The interviewees held leadership positions in their particular fields and they were chosen for their accessibility and their ability to provide insightful comment on –

a. the requirements of intelligence-sharing for customs purposes;

b. the practical application of the proposed legal framework; and

c. the practicalities of maintaining customs intelligence-sharing relationships.

Interviews were conducted with individuals who held the following positions:[28]

**Table 1. Interviews**

| Interviewee | Role | Interview date |
|---|---|---|
| **One** | Intelligence and law enforcement operations and international relations in a border agency | 27 May 2013 |
| **Two** | Legal counsel in a border agency | 4 June 2013 |
| **Three** | Law enforcement and intelligence operations in a policy agency | 9 June 2013 |
| **Four** | Intelligence and law enforcement operations and international relations in a border agency | 27 May 2013 |
| **Five** | Intelligence analysis and international operations in a border agency | 27 May 2013 |
| **Six** | Intelligence, defence and international operations in a security agency | 8 June 2013 |
| **Seven** | Intelligence and law enforcement operations in a border agency | 5 June 2013 |
| **Eight** | Legal counsel in a border agency | 9 June 2013 |
| **Nine** | Intelligence and law enforcement operations in a border agency | 12 June 2013 |
| **Ten** | Legal counsel and policy advisor in a policy agency | 13 May 2014 |

The interview sample size is small. This reflects the small size of both New Zealand's intelligence community and of the group that has expertise in customs intelligence issues.

The interviews complied with the University ethics requirements. The questions were written to conform to the requirements of the Ethics Committee.

[28] Refer to Appendix One for the Human Ethics Committee consent form and the interview questions.

Personal and agency anonymity was a requirement for the interviewees' participation, for security reasons and to protect international relationships.[29]

#### *F Stage V: Conclusion*

The work closes in Chapter Eight with conclusions on the suitability of the legal framework.

## *III Scope*

A legal framework is proposed to show how the existing single window can be extended to include intelligence-sharing. It includes requirements for the treatment of human rights to improve public confidence in the intelligence-sharing process. It does not undertake a survey of all intelligence-sharing tactics to determine whether any other approach to intelligence-sharing is preferable.

Some states have single window systems for sharing transaction information and a large number of states already have agreements in place for customs cooperation and intelligence-sharing. However, there is no system to automatically and electronically share customs intelligence. A single window system could also be used for this purpose.

The proposed framework enables a distributed model for intelligence-sharing, so each customs administration can share intelligence directly with another customs administration. This method of direct exchange between two customs administrations replicates and automates the existing manual processes for intelligence-sharing. It does not create a central monolithic repository of intelligence to which states can subscribe.

The legal framework does not include domestic law for establishing a single window or connecting national single windows with one another. The WCO and the United Nations Commission on International Trade Law (UNCITRAL) member states are already researching the legal aspects of implementing a single window.[30] This research focuses on the use of law to enable a uniform approach to sharing intelligence in support of single window processing, where international single windows have been implemented. This is proposed as an alternative to the current intelligence-sharing practices that include numerous bilateral agreements between states.

To clarify the purpose of the legal framework, the information needs of government intelligence users were considered. All sources of intelligence used in trade risk-

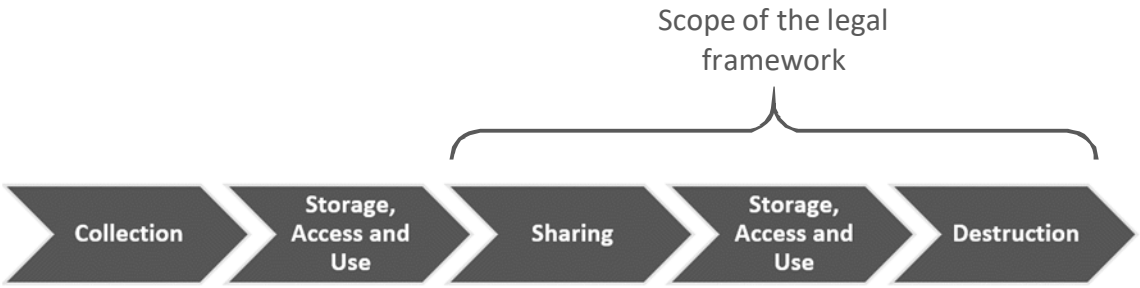
[29] It may be noted that publishing the identity of some intelligence personnel is prohibited by the Intelligence and Security Act 2017 (New Zealand), s 227.

[30] *Recommendation No. 36: Single Window Interoperability* ECE/TRADE/C/CEFACT/2017/6 ; *Recommendation No. 35: Establishing a legal framework for international trade Single Window* ECE/TRADE/401 (2010); and *Joint WCO/UNCITRAL Working Group on Model Legal Guidelines for Implementation of Integrated Border Management* PC0197E (2007).

management are considered. This includes intelligence gained and used in other settings, such as intelligence used for immigration decision-making. For example, intelligence about the international movements of people and the businesses and people with whom they associate is useful when assessing the risk associated with the goods they trade. For this reason, the legal framework must include provision for sharing information from sources other than customs transactions for trade risk-management purposes.[31]

This legal framework addresses the sharing and subsequent access to and use of intelligence following its collection. It also addresses issues relating to the management of information after it has been shared. It is not aimed at issues relating to the act of collecting or obtaining intelligence at its source. However, human rights treatment during the acquisition of intelligence does have a bearing on public confidence and trust. For that reason, collection issues are discussed in relation to trust in customs and government intelligence activities in general.

**Figure 1. Intelligence lifecycle**




Other uses for intelligence exchanged through the single window system are not proposed here. The proposed legal framework focusses on automating existing intelligence exchanges between customs administrations for customs purposes. Use of this same intelligence by other government agencies and for other purposes would conflict with the Purpose Specification and Use Limitation privacy principles. [32] If the legal framework is used to share information for too broad a range of purposes, that would create downstream privacy risks. For example, it may be difficult or impossible to determine when the information is no longer required for all of the purposes and can be deleted. Different purposes should require additional enabling legislation so that the control and use of information can be weighed and allowed or disallowed in context.

In practice, there can be no guarantees that the parties will honour the rules that are put in place in the legal framework. The absence of guarantees is due to the apparent

[31] For example, information about criminal convictions or false immigration declarations.

[32] OECD Privacy Framework, above n 12. Purpose Specification and Use Limitation are privacy principles in the OECD Privacy Framework, discussed in Chapter Four.

reluctance of any law enforcement or intelligence agencies to allow an independent third party or foreign agency to review its intelligence material or practices.[33]

Interviews were conducted with experts in the field of customs intelligence, law enforcement operations, privacy and international relationships in New Zealand.

The WCO Data Model or other WCO standards should be extended to include the specific intelligence data elements that might be shared and the format to which they should conform.[34] An overview of the likely scope of these data elements is included in Chapter Two.

## *IV The Single Window*

This Part discusses the single window system, which is an electronic information exchange system used by customs administrations. It proposes a legal framework for sharing intelligence through this system and shows how it can include evident treatment of human rights.

There are five sub-parts in this Part. Sub-part A explains why single window systems are used by customs administrations. Sub-part B describes the way in which single window systems provide a single communications interface between a trader and multiple government agencies. It also explains how the single window systems of states can be connected to each other to exchange information for the end-to-end automation of an international (export and import) trade transaction. The progress made by some states to implement single window systems is discussed in sub-part C.

In sub-part D, the possibility of using the single window system to share intelligence is raised. Sub-part E discusses the potential benefits of sharing intelligence with other states through the single window system.

### *A Why Single Window Systems are Needed*

The single window concept is an initiative of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and the WCO.[35] The World Trade Organisation (WTO) Trade Facilitation Agreement mandates that all members of the

[33] Intelligence material can have restrictive handling caveats. For example, the Five Eyes intelligence partners, New Zealand's closest intelligence relationship, might hold intelligence material that is variously labelled "NEW ZEALAND/AUSTRALIA EYES ONLY", or "UK/USA EYES ONLY". The existence of restrictions like this makes it unlikely that a third party would be granted permission to review all intelligence material and practices within a state agency.

[34] WCO "WCO Data Model" (2008) World Customs Organisation <www.wcoomd.org>.

[35] UN/CEFACT, *Recommendation No. 33: Recommendation and Guidelines on establishing a Single Window*, above n 4.

WTO shall endeavour to establish a single window to enable traders to submit documentation for the import and export of goods through a single entry-point.[36]

The WCO is an international body that helps its member governments communicate and co-operate on customs issues. It claims that:[37]

> Today, the WCO represents 182 Customs administrations across the globe that collectively process approximately 98% of world trade. As the global centre of Customs expertise, the WCO is the only international organization with competence in Customs matters and can rightly call itself the voice of the international Customs community.

With a single window system, parties conduct cross-border trade transactions by electronically lodging information through a single entry-point to all government agencies. This fulfils both import and export regulatory requirements. A single window reduces compliance costs for businesses and increases efficiency by reducing the duplication of information lodged with government.[38]

Internationally, customs administrations have implemented these systems to simplify and streamline customs processes and to save time and money.[39] This sub-part explains why some states have implemented single window systems to connect the electronic systems of their border agencies in order to improve the sharing of information and coordination of processes.[40] Other states have taken steps to create an international single window system that connects their national single window systems with the single window systems of other states.[41] In the following text, the term "single window" is generally used in the context of sharing information internationally between single window systems.

---

[36] WTO "Preparatory Committee on Trade Facilitation, Agreement on Trade Facilitation WT/L/931" (15 July 2014) United Nations Economic Commission for Europe <tfig.unece.org> and WTO "Bali Ministerial Declaration and Decisions" (27 November 2014) WTO <www.wto.org>.

[37] "WCO In Brief" (12 November 2017) World Customs Organisation <www.wcoomd.org>.

[38] See, for example, OECD "Quantitative Assessment of the Benefits of Trade Facilitation TD/TC/WP (2003) 31/FINAL" (13 November 2003) OECD <www.oecd.org> and Trisha Rajput and Abhinayan Basu Bal "Chapter 16 - Creating Sustainable Global Supply Chains through Single Window and Paperless Trade Initiatives: Efforts of WTO and UNCITRAL in Perspective" (unpublished chapter in book Yves-Louis Sage (ed) "Harmonising Trade Law to enable Private Sector Regional Development", 7 November 2017).

[39] For examples see European Commission and Malta Customs, above n 6.

[40] See New Zealand Customs Service "Statement of Intent 2012-2015" (2015) New Zealand Customs Service <www.customs.govt.nz>, at 21 and Aphichat Aumyoo "ASEAN Single Window Initiative" (18 July 2013) New Zealand Ministry of Foreign Affairs and Trade <www.mfat.govt.nz>.

[41] Aumyoo, above n 40.

Single window systems could be usefully used to share intelligence about the trade transactions they process. However, to date no single window system is used as a mechanism for sharing customs intelligence between states. There are no other automated systems to share the trade intelligence used by border agencies when making decisions on what people, goods and craft may cross the border.

Intelligence contributes to national and collective international security and compliance goals. As noted by Garcia, there is now an opportunity to make advances in intelligence-sharing to improve governments' responses to shared threats:[42]

> Currently, military, defence and security policies are reactive, rather than preventative. The time is ripe for a re-look at how multilateral cooperation and information-sharing is really conducted within the hemisphere, more importantly at the strategic and operational levels.

It is concluded that the ability of customs administrations to collect and process information to manage trade risk will improve through the use of new single window technology. Increased information-sharing, by including intelligence with trade transaction information, will help customs administrations to risk-manage trade transactions more effectively in the new single window systems they are developing. A common legal framework could enable intelligence-sharing through single window systems.

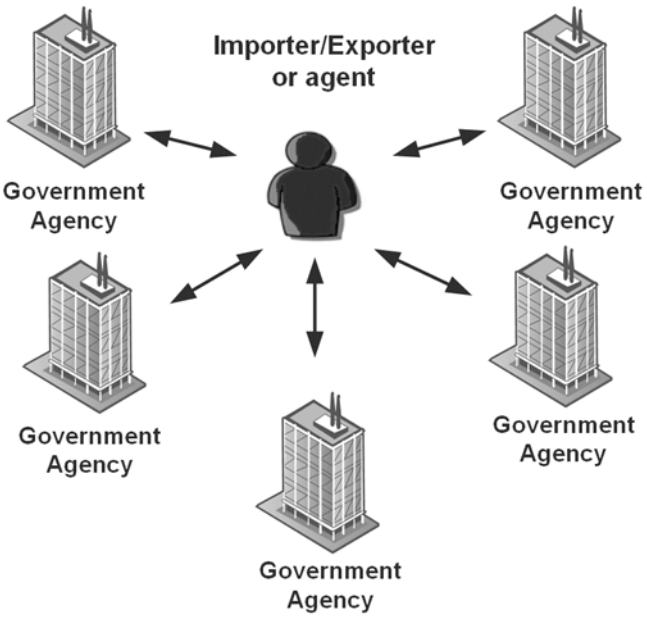
Chapters Two, Three and Four identify the criteria for a common legal framework to enable better risk-management of the transactions that are processed in a single window system. The sub-part below explains how a single window is used to process the trade transaction information.

### *B How the Single Window Works*

The single window is a system in which the parties involved in border transactions electronically lodge standardised information through a single entry-point to fulfil all import and export regulatory requirements. In states without a single window, importers, exporters, customs brokers and logistics and shipping companies are required to lodge information separately with all the government agencies involved at the border. Much of this information, such as the parties involved and the manifest, may be repeated in each lodgement. This is illustrated in Figure 2.

[42] Garcia, above n 23, at 10.

**Figure 2. Border transactions without a single window**




*C Extent of use*

It is not easy to find material from which it is possible to deduce the extent to which single window systems have been implemented. In 2011 the WCO reported the findings of a survey of single window implementation by WCO member states. The survey asked how many government agencies were involved in the cross-border movement of goods. Of the 58 member states that completed the survey[43]:

(a) 58% (32) indicated fewer than 16 government agencies are involved;

(b) 29% (16) indicated 16 to 30 government agencies are involved; and

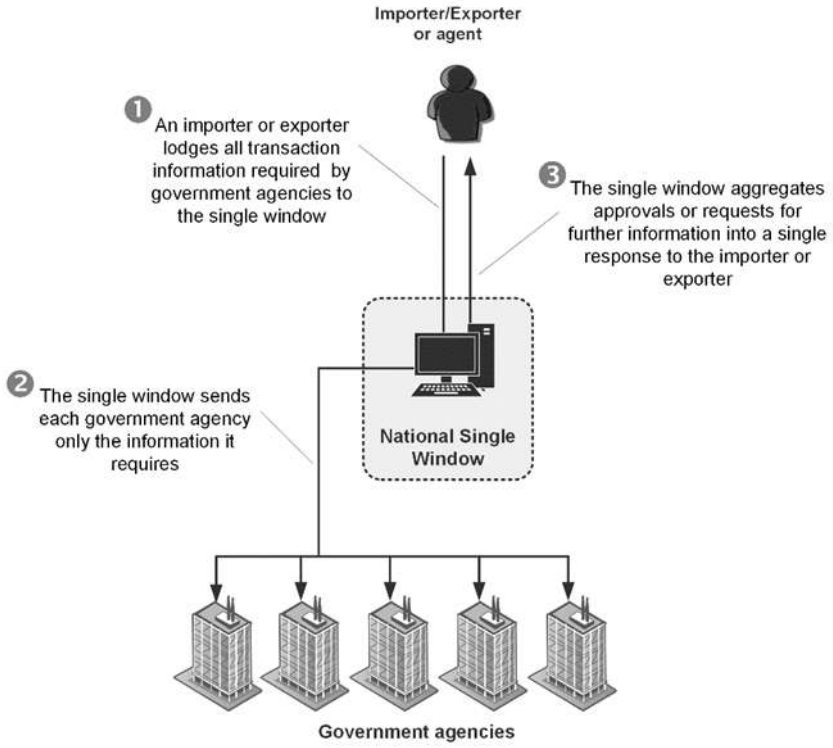
(c) 13% (7) indicated more than 30 government agencies are involved.

In a domestic context, a single window will reduce compliance costs for businesses and increase efficiency by reducing the need to submit transaction information separately with multiple government agencies. Information is provided only once, through a single government entry-point (the single window).

A single window is illustrated in Figure 3.

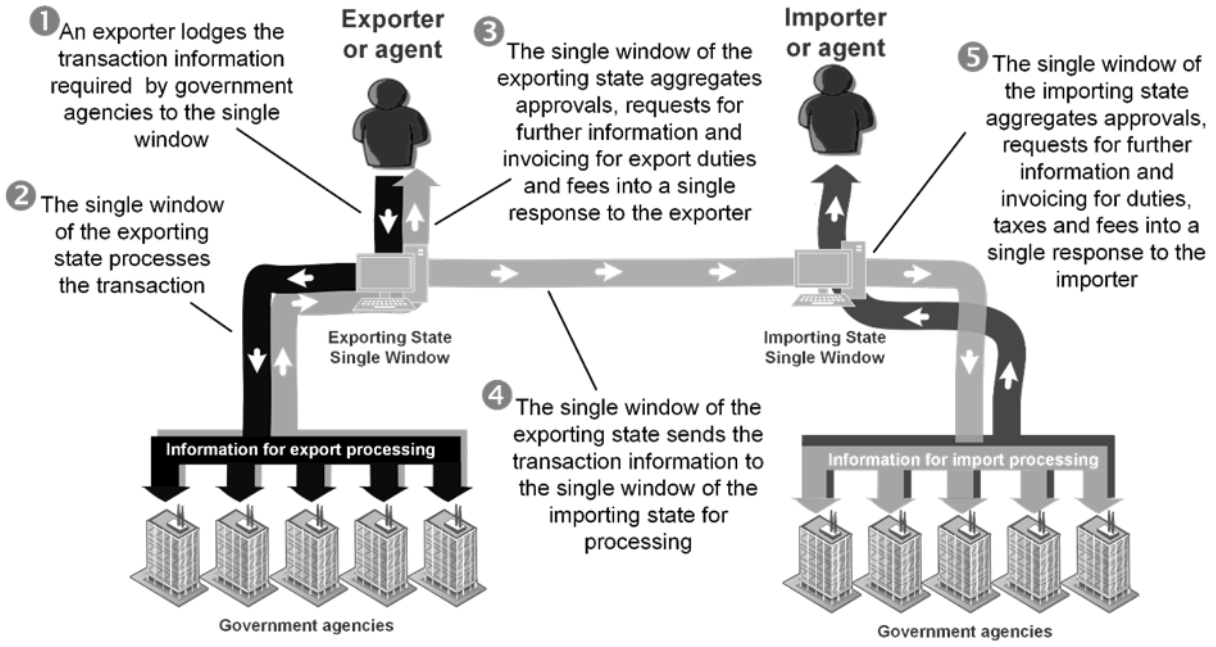
[43] WCO, above n 13. The WCO has not published a more recent survey.

**Figure 3. Border transactions in a single window environment**



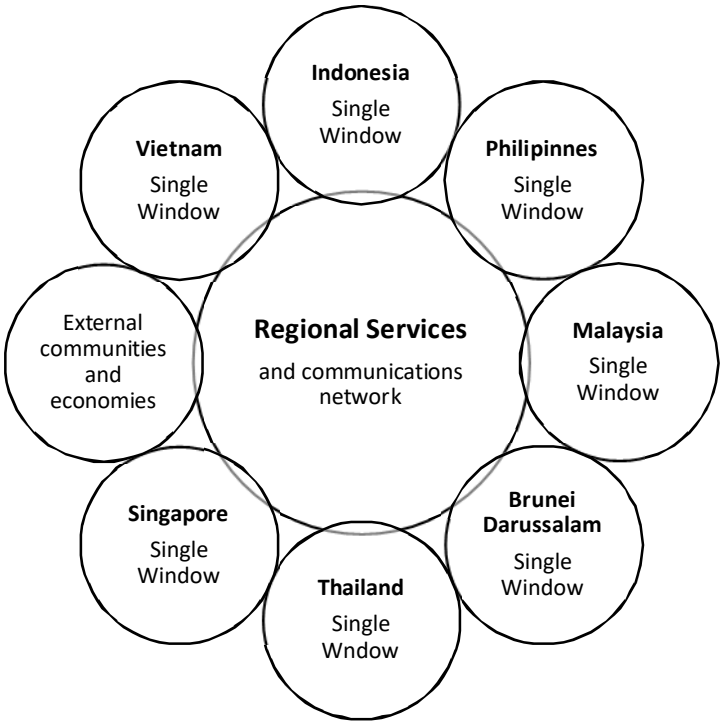

In the international context, an exporting state's national single window can share the transaction information in a standardised format with an importing state's national single window to gain further efficiencies in supply chain processing. Figure 4 illustrates how this works.

**Figure 4. The international single window concept**



The diagram below illustrates a pilot international single window programme that is aimed to connect the national single windows of the Association of South East Asian Nations (ASEAN) states.[44] In this pilot project, importers will not need to submit information already lodged with the exporting state's national single window system.

**Figure 5. ASEAN single window Pilot Project 2011-2013**




*D State Implementations*

Many states have implemented, or are in the process of implementing, a single window system. This sub-part outlines global progress. The WCO survey of single window implementation reports that 19 of 58 survey respondents (34%) claim to operate a single window system.[45] It reports that many of those single window systems are recent developments, with 9 respondents bringing their single window systems into operation between 2006 and 2010.

The EU began work to implement a single window for member states after 2013.[46] The most recent report available from the European Commission is the 2016 E-Customs

[44] Image adapted from Aumyoo, above n 40. In October 2017, ASEAN was still reporting on its website that Brunei and Vietnam were expected to join the ASEAN single window by mid-2017 at Association of South East Asian Nations "What is the ASEAN Single Window?" ASEAN (24 October 2017) <asw.asean.org>.

[45] WCO, above n 13. Only 7 states have published references to their national single window systems (the most recent being in 2010) on the WCO website at WCO "Activities and Programmes: National Single Window" (15 November 2017) World Customs Organisation <www.wcoomd.org>.

[46] European Commission, above n 6.

Report published on 10 July 2014 which stated a single window system was in use by seven Member States.[47]

Raus described a number of facilitators and barriers related to the EU implementation of a single window system.[48]

**Table 2. Facilitators of, and barriers to, single window implementation**

| *Facilitators of adoption* | Barriers to adoption |
|---|---|
| 1. *Benefit potential for the public sector* | 1. Slowdown in regulations execution<br>2. due to missing procedural templates |
| 2. *Procedural improvements and*<br>3. *streamlined business processes* | 3. Increased complexity in the<br>4. standardization process itself |
| 4. *Avoidance of misinterpretations of standardised regulations* | 5. Computerisation of operations |
| 5. *Standardisation of processes, messages, and data model* | |

The ASEAN member states agreed to create a regional single window in 2005.[49]

In the United Kingdom an inter-departmental web portal has been implemented to provide tools and information on international trade regulation. It also provides a web-based service for export licence applications that integrates information requirements of HM Revenue and Customs Service and the Department for Business, Enterprise and Regulatory Reform. These developments are the first steps in the plan for providing traders and freight forwarders with a single interface for entering all the information required by government for international trade transactions.[50]

Similarly, Indonesia completed its third phase of a single window implementation in December 2008. The development integrated the information systems of government authorities to allow all 4,582 registered importers to deal with these authorities electronically.[51] It included systems for information to be submitted simultaneously to

[47] *e-Customs Progress Report* TAXUD.A.3(2017)3921405 (2016), at 14.

[48] Marta Raus, Barbara Flugge and Roman Boutellier "Electronic Customs Innovation: An Improvement of Governmental Infrastructures" (2009) 26 Government Information Quarterly 246, at 249.

[49] Tsen, above n 14. The ASEAN single window was planned to be in place by 2015 but it has not yet been fully implemented, according to Association of South East Asian Nations "What is the ASEAN Single Window?" ASEAN (24 October 2017) <asw.asean.org>.

[50] United Kingdom National Audit Office *HM Revenue & Customs' Transformation Programme: Report* (The Stationary Office, London, 2008), at 30.

[51] Embassy of the Republic of Indonesia "Trade and Investment News" (30 December 2008) Embassy of the Republic of Indonesia <embassyofindonesia.org>.

the government authorities and integrated the business processes for customs control, licencing, payments and logistical systems and other export-import handling systems.[52] This implementation is part of a broader plan for Indonesia to participate in an ASEAN single window system.[53]

The Australian Customs and Border Protection Service, like many authorities, has yet to meet all the requirements of UN/CEFACT recommendation 33.[54] In 2005, Australia began a piecemeal implementation of a single window, called the Integrated Cargo System (ICS), which integrates Australian customs information systems with those of other government agencies.[55] By June 2009 the ICS was in place and processing transactions for the Australian customs service but it was not operating as a single window system because:[56]

> Achieving a whole-of-government international trade single window by facilitating the issuing of government import/export permits through the ICS would require substantial investment due to the diversity and complexity of government permits processes.

The Australian customs administration did not begin a full single window development, stating that it would develop capabilities "where the cost-benefits are clear" to enable "information able to be accessed and used by multiple government agencies".[57]

The Asia Pacific Economic Cooperation (APEC) forum has a Sub-Committee on Customs Procedures (SCCP). In 2010, it reported that thirteen SCCP member states had completed the implementation of a single window: Australia; Brunei; Canada; Chile; China; Indonesia; Japan; Republic of Korea; Malaysia; Philippines; Singapore; Thailand; and the United States of America.[58]

---

[52] Brunei FM "Indonesia: President Commissions Single Window Export-Import Service" (30 January 2010) Brunei FM <news.brunei.fm>.

[53] Embassy of the Republic of Indonesia "RI to Take Advantage of ASEAN Single Window System" (19 September 2010) Embassy of the Republic of Indonesia <embassyofindonesia.org>.

[54] UN/CEFACT, above n 35.

[55] Justin Malbon and Bernard Bishop *Australian Export* (2nd ed, Cambridge University Press, Melbourne VIC, 2014), at 194 and SCCP *Working Towards the Implementation of Single Window within APEC Economies: Single Window Development Report APEC#207-CT-01.7* (Australian Customs Service, Canberra, 2007) at 57.

[56] Australian Customs and Border Protection Service "Enhanced Trade Solutions 2015" (12 November 2017) Australian Customs and Border Protection Service <www.border.gov.au>, at 7.

[57] At 11.

[58] *SCCP Single Window Report: Working Towards the Implementation of SW in the APEC Economies and International Interoperability* 2010/SOM3/SCCP/002 Agenda Item: 4(ii). Note that this report conflicts with statements made a year earlier that indicated Australia had not and did not intend to complete a full single

Non-APEC states operating a single window include Finland, Germany, Ghana, Guatemala, Mauritius, Senegal and Sweden.[59] In some states, such as Sweden, use of a single window system is voluntary.[60] Importers and exporters can choose to interact with customs administrations and other government agencies through other means, such as paper-based systems. In other states such as Finland and Senegal, use of the single window system is mandatory.[61]

The interconnection of national single window systems to create international single windows affords an opportunity to also use the system for intelligence-sharing. The next sub-part discusses how the system might be used.

### *E How the Single Window System might be Used*

Many states are implementing, or have implemented, a single window system. As explained in sub-part B, a single window system enables the exchange of all the data necessary for a customs administration to process an inbound or outbound trade transaction. This sub-part outlines the potential for intelligence-sharing through single window systems and the benefits this might produce. The benefits include improved compliance with customs law and the prevention of terrorism and other transnational crime. The discussion in the following Chapters has a strong focus on terrorism. This is because terrorism has been a major security focus of customs and other law enforcement agencies since the 9/11 terrorist attacks in the United States. Many of the examples of privacy and human rights abuses discussed below involve the use of intelligence in counter-terrorism activities. Government agencies like the New Zealand Customs Service have exemptions from privacy law for information used for security purposes such as counter-terrorism.

The customs administration obtains information directly from the trader in some cases. In other cases, the trader completes the import or export through an intermediary such as a courier, mail or freight logistics company. Exporters and intermediary companies may share information directly with the customs administration if they are part of an Authorised Economic Operator (AEO) scheme.[62] New Zealand and the United States

window implementation. See Australian Customs and Border Protection Service, above n 56. APEC has not published a more recent report of single window implementations.

[59] UN/CEFACT, *Case Studies on Implementing a Single Window: To Enhance the Efficient Exchange of Information Between Trade and Government* [Working Draft] (UN/CEFACT, Brussels, June 2006).

[60] At 72.

[61] At 11 and 54.

[62] *Authorised Economic Operators: Guidelines* TAXUD/B2/047/2011–Rev.5 (2014) and WCO "The Authorised Economic Operator and the Small and Medium Enterprise" (May 2010) World Customs Organisation <www.wcoomd.org>.

operate an AEO system called the Secure Export Scheme (SES) under which the states examine and certify the security of the exporter and its intermediary's premises and processes.[63] In the United States, exporters and intermediaries may also be part of an AEO system called the Customs-Trade Partnership Against Terrorism (C-TPAT).[64] Membership in these AEO systems enables traders to provide import and export services with minimal intervention by government.[65]

However, these AEO systems provide no additional information about each transaction for risk-assessment other than that which is usually submitted electronically.[66] Small and low value items, such as mail, travel within larger consignments and may not be reported.[67] These smaller items may have customs declaration information attached that is not collected electronically.[68] Consequently, import or export as a mail item is a technique commonly used by criminals.[69] Courier, mail or freight logistics companies may have information about importers and exporters of large volumes of items to which customs administrations do not have access. In future, businesses could provide that information to customs administrations through a single window system.

No single window system is currently used to exchange intelligence information. Also, while each single window system uses a common format for the data elements included in the trade transaction, there is no similar format for the exchange of intelligence

[63] New Zealand Customs Service "Secure Export Scheme" (2015) New Zealand Customs Service <www.nzcs.govt.nz>.

[64] United States Customs and Border Protection Service "C-TPAT: Customs-Trade Partnership Against Terrorism" (2015) United States Customs and Border Protection Service <www.cpb.gov>; Kati Suominen *Fueling the Online Trade Revolution: A New Customs Security Framework to Secure and Facilitate Small Business E-Commerce* (Rowman & Littlefield, Lanham MD, 2015), at 12 and Peter Mento *C-TPAT and ISA, Understanding the Effectiveness of Trade Partnerships for Customs Enforcement* (Lulu Press, Raleigh NC 2004), at 11.

[65] DHL Global Forwarding "DHL Global Forwarding Ocean Freight: Beyond Port to Port" (2015) Deutsche Post DHL Group <www.dhl.co.nz>, at 2 and 3.

[66] New Zealand Customs Service "Import Entry Process" (9 July 2015) New Zealand Customs Service <www.customs.govt.nz>.

[67] For example, see Montserrat Customs and Excise Department "A Guide to Clearing Air Cargo Through Customs " (2008) Montserrat Customs and Excise Department <customs.gov.ms>, at 3 and Estonian Tax and Customs Board "Customs Formalities Applied with International Postal Consignments" (2012) Estonian Tax and Customs Board <www.emta.ee>, at 2.1.

[68] Her Majesty's Revenue and Customs Service "Notice 143: A Guide for International Post Users" (1 February 2014) Her Majesty's Revenue and Customs Service <www.gov.uk>, at 2.1.

[69] Klaus von Lampe "The Practice of Transnational Organized Crime" in Felia Allum and Stan Gilmour (eds) *Routledge Handbook of Transnational Organized Crime* (Routledge, Abingdon, 2012) 186, at 196 and United States General Accounting Office *Money Laundering and Currency: Smuggling: An Assessment* (DIANE Publishing Company, Washington DC, 1994), at 28.

information. This is evident in the analysis of international agreements included in Chapter Five.

A standardised international legal framework is needed to facilitate effective and harmonised arrangements for intelligence-sharing within a single window system. A real-time system for sharing intelligence which associates that intelligence with trade transactions will enable consistent and more effective risk-management at the border by all states.

There are risks that such a system will infringe human rights and privacy law. The immigration case of *Zaoui v Attorney-General* suggests that intelligence-sharing can present difficulties when judicial decisions rely on information supplied in confidence by other governments.[70] So, a process should exist through which issues about personal information can be resolved quickly and without reference to a court. There are also risks that such a system might accidentally disclose personal information or be manipulated by governments to impede the legitimate movement of people, goods and craft for economic or political advantage. These risks need to be managed.

## *V The Contribution to Knowledge*

This research contributes to knowledge in the field of law relating to international agreements and the sharing of information for law enforcement purposes. It aims to enrich academic knowledge and the understanding of the importance of including clear rules for information-sharing when the existence of that information must remain secret.

The proposed legal framework will enable customs administrations to share intelligence through a single window system for risk managing the trade transactions that are processed through the same system. No existing legal framework enables the real-time, electronic exchange of intelligence information for trade risk-management with clear terms for the control of that information.

### *A Privacy*

The proposed legal framework bridges the gap between the law that exists for the control of personal information and the need for transparency in international information-sharing agreements.

Presently, there is a body of Common Law and legislation and international instruments that set out expectations for the treatment of privacy and other human rights.[71] Many of

[70] *Zaoui v Attorney-General (No 2)* [2005] NZSC 38, [2006] 1 NZLR 289. This case is discussed further in Chapter Three.

[71] Discussed in Chapter Four.

the current international arrangements for customs intelligence-sharing do not fulfil these expectations.

Public concern about the secrecy of government information-sharing arrangements for law enforcement and national security has been regularly publicised by the media.[72] That concern has increased as a result of revelations about the abuse of human rights by governments for law enforcement and national security purposes.[73] Public confidence is eroded by government secrecy. Democratic governments rely on public support, so it follows that secrecy is harmful to democratic governments. Poor public confidence is an impediment to intelligence cooperation between states.

#### *B Transparency*

In New Zealand, the Office of the Ombudsmen and the Office of the Privacy Commissioner exist to investigate complaints against government agencies.[74] However, secrecy in information-sharing agreements makes it difficult for individuals to discover and complain about the use of their personal information. Furthermore, although the Ombudsmen and Privacy Commissioner have powers to investigate complaints against New Zealand agencies, they have no powers to enforce compliance with any law.[75] They also have no power to investigate complaints against the agencies of foreign governments with which intelligence may be shared.

The proposed legal framework will improve public confidence in the secret intelligence work of customs administrations. It does this by making the terms for handling personal information evident. This clarity provides the public with confidence that human rights will be protected even when the existence of personal information is kept secret from the information subject.

### *VI Potential Benefits*

The product of this research is a method for sharing intelligence through a single window system. This offers significant direct and indirect benefits for New Zealand. Customs administrations share and use trade and security intelligence to meet their responsibilities for border security, economic security and pandemic control.[76] International intelligence-sharing, through the proposed legal framework will provide the following benefits.

---

[72] Discussed in Chapter Two and Chapter Four.

[73] Discussed in Chapter Four.

[74] Ombudsmen Act 1975 (New Zealand), s 13 and Privacy Act 1993 (New Zealand), s 13.

[75] Ombudsmen Act 1975 (New Zealand), ss 22-24 and Privacy Act 1993 (New Zealand), s 77.

[76] Andrew Ladley and Nicci Simmons *Conceptualising the Border and Customs in the 21st Century - or How to Outfox the Future* (Institute of Policy Studies, Wellington, 2007), at 7.

1. Uniform terms for intelligence-sharing: Numerous bilateral and multilateral agreements exist for intelligence-sharing purposes. The terms in these agreements for the treatment of information are various. Updating these agreements with a single, uniform set of terms for how information should be treated will improve certainty and public confidence in the way information is treated.
2. Lower compliance costs for business: Better intelligence-sharing will enable the government to focus interventions on the highest risk transactions, thereby reducing compliance costs and delays for businesses.[77]
3. Better privacy and confidentiality: Individuals and businesses will benefit from clear terms for the use and protection of confidential commercial information and private personal information in intelligence-sharing relationships. This will help protect business profitability, privacy and human rights.
4. Less crime: The legal framework will make intelligence available more quickly to New Zealand's border agencies. This will help the government to investigate and prosecute crimes such as human trafficking and the trade of illicit drugs, weapons, unsafe goods, endangered species and child pornography. This intelligence will also be used to combat country of origin falsification and other fraud designed to evade taxes, quotas and customs duty.
5. Improved intelligence-sharing: Current intelligence-sharing arrangements are very reliant on trust between the individual staff members that exchange that intelligence.[78] A single window system with built-in rules for enabling the exchange and control of intelligence will enable the sharing of larger volumes of information than these individuals can manage, once trust has been established between the participating states. Shared intelligence contributes to collective security through a 'melding' of security and intelligence activity.[79]
6. New agreements can be made more speedily: Benefits for government stem from the uniformity of terms for border security intelligence-sharing. This makes the formation of intelligence-sharing agreements simpler and faster. This also reduces the likelihood of misunderstandings and disputes.

[77] WCO and UNCTAD *Risk Management in Customs procedures* (UNCTAD, Geneva, 2008), at 2. See also Catherine Truel *A Short Guide to Customs Risk* (Gower, London, 2010), at 6.

[78] Discussed in Chapter Two.

[79] Clive Walker and Andrew Staniforth "The Amplification and Melding of Counter-Terrorism Agencies: From Security Services to Police and Back Again" in Aniceto Masferrer and Clive Walker *Counter – Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State* (Edward Elgar, Cheltenham, 2013) 293, at 293-319.

## *VII Chapter Summary*

Chapter One has set out the logic of this thesis, which is -

1. there is no law enabling customs to share intelligence electronically and in real-time for risk management purposes; and
2. the privacy principles of the OECD Privacy Framework are the most widely accepted expression of public expectations for the treatment of privacy; and
3. with some exceptions, the principles of the OECD Privacy Framework can be imposed as controls on a practical intelligence-sharing arrangement; and
4. making those controls transparent will improve public confidence; so
5. a legal framework that allows customs administrations to share intelligence through the transactional single window system, and at the same time show how privacy and other human rights are treated, will improve public confidence.

Along with describing the thesis, this introductory Chapter has described the single window system and the potential benefits of sharing customs intelligence through a single window system. The benefits include savings for governments and traders.

The thesis does not include a prediction of the public acceptance of the legal framework. The acceptability of the privacy controls and other terms of the legal framework would be determined in other forums, such as in the parliamentary debating chamber, select committees and in court cases. These forums include public scrutiny and debate which has not occurred for many existing intelligence-sharing agreements.

The method that was followed to develop the proposed legal framework was described. The method involved:

1. establishing the criteria for the legal framework that would enable customs administrations to share intelligence through a single window system.;
2. establishing the human rights which, if prudently treated, should lead to improved public confidence in intelligence-sharing;
3. evaluating the existing agreements and models to demonstrate that no current legal frameworks can meet the needs described in points 1 and 2 above; and
4. developing a legal framework for sharing intelligence through a single window system and evaluating that framework against the same criteria.

The method is implemented in the following seven Chapters.

Chapter Two includes an overview of the technical and operational information requirements for a customs intelligence-sharing system. It discusses the reasons why much of the information must remain secret and some of the harms that can occur as a result of that secrecy.

Chapter Three describes the privacy and human rights that should be protected by an intelligence-sharing system and provides some insight into the harms that can occur if these rights are not adequately protected.

Chapter Four develops the discussion of privacy rights and the impact of the 9/11 terrorist attacks and the Snowden leaks on the treatment of privacy by governments. Chapter Four offers a model for understanding the harms that can be caused by breaches of these rights. The principles of OECD Privacy Framework are acknowledged as the most widely accepted statement of public privacy expectations and they are indicated for inclusion, wherever possible, in the legal framework that is developed in later Chapters.

Chapter Five lists a set of measures based on the requirements discussed in Chapter Two, Chapter Three and Chapter Four. It summarises the evaluation of existing customs information-sharing agreements as well as some other information sharing models against these measures. The evaluation shows that there is no existing legal framework that would enable customs administrations to share intelligence through a single window system. The Chapter discusses a small selection of these agreements in more detail to illustrate the extent to which the measures are typically implemented.

Chapter Six outlines the legal framework, a draft international convention and a model domestic law, that was developed to enable customs intelligence-sharing through a single window system. Appendices II and III contain the full text of the international convention and a model domestic law.

Chapter Seven evaluates the proposed legal framework against the measures set out in Chapter Five. It also summarises the feedback from the experts who were interviewed for their views on whether the legal framework would be practical and effective for their needs.

Chapter Eight provides conclusions on the suitability of the legal framework for automating customs intelligence-sharing through a single window system.

# Chapter Two – Information, Secrecy and Public Confidence

The thesis is that, with an appropriate legal framework, the single window could be used to automate intelligence exchanges. The objective of this Chapter is to build on the background to single window systems provided in Chapter One. This Chapter provides an overview of the types of information that need to be covered by a legal framework that enables customs intelligence-sharing through a single window system. It identifies the essential operational requirements that customs administrations have for sharing intelligence. It describes the customs risk assessment process, the kinds of information needed in that process and the information standards that are currently used.

The risk assessment process helps customs administrations to meet their responsibilities for law enforcement relating to the cross-border movement of people, goods and craft. These responsibilities include aspects of national security. The Chapter also describes the need for secrecy in customs intelligence-sharing and introduces some of the reasons why this secrecy can erode public confidence. In order to protect the security of intelligence and law enforcement processes, some types of information and information sources are excluded from the discussion. Some issues encountered in other intelligence and policing cooperation arrangements and their relevance to the proposed legal framework are introduced in the last Part of this Chapter to provide some insight about the intelligence-sharing context.

This Chapter is arranged in eight Parts. Part I explains how the risk-assessment process used by customs administrations is part of an approach to collective law enforcement and security. Part II identifies some of the types of information used and shared by the state for trade risk-management. Part III describes the national security role that customs administrations perform for the state. The security and law enforcement objectives that the state seeks to achieve through its customs administration and other agencies are discussed in Part IV. Part V explains why the intelligence used for these purposes must remain secret. The tension between that secrecy and the state's need to maintain public confidence is described in Part VI. The proposed legal framework enables the use of single window systems to automate existing intelligence-sharing arrangements. There are other factors that must be addressed if the legal framework is to be used in the establishment of a new intelligence-sharing agreement. Part VII introduces some of those other factors. This Chapter is summarised in Part VIII.

## *I The Risk-Assessment Process*

This Part describes the way in which customs administrations use intelligence to assess transactions and target resources for further investigation or intervention.[80] It provides the background reasons for the kinds of information that are required in a model to share intelligence through a single window system. This Part provides a general outline of the risk-assessment process. It does not examine the quality of, nor make normative statements about, customs risk-assessment processes

Customs administrations use information to determine whether the transactions present a low or acceptable level of risk of non-compliance with customs laws or other regulations that the customs administrations must enforce.[81] Indicators of high risk transactions include among other things, no labelling on packages and the declared value being excessively low in relation to the number or type of items and unusual combinations of products.[82] Typically, the processing of low risk transactions is automatically completed. Transactions deemed high risk receive targeted intervention, which is usually a physical inspection of the goods being transacted. An intervention threshold is set for transactions deemed to be of a moderate risk. Moderate risk transactions receive varying treatment depending on trends such as whether the risk is increasing or decreasing, whether supplementary information is available, and whether or not customs resources are available to undertake the intervention. The decision to intervene with moderate risk transactions is based on cost, resource availability, and potential benefit.[83] The benefits of intervention are that illicit activity or goods are intercepted, additional revenue is collected, or information is gained that contributes to future risk-assessments.

The proportion of transactions deemed to be of moderate risk may receive further attention to quantify the level of risk based on whatever supplementary information is available.[84] Typically, only a small proportion of transactions is considered to be high risk and receive intensive intervention. There is also regular sampling of low risk

[80] The use of intelligence by governments to target resources in the post-9/11 fight against terrorism is discussed in Clive Walker "Keeping Control of Terrorists without Losing Control of Constitutionalism" (2007) 59 Stan L Rev 1395, at 1396.

[81] Iordache and Voiculet, above n9, and Truel, above n 77, at 22.

[82] European Commission, above n 17, at 47. More detailed lists of risk indicators are restricted to WCO members but are referred to in the index of the WCO Customs Risk-Management Compendium, above n 17.

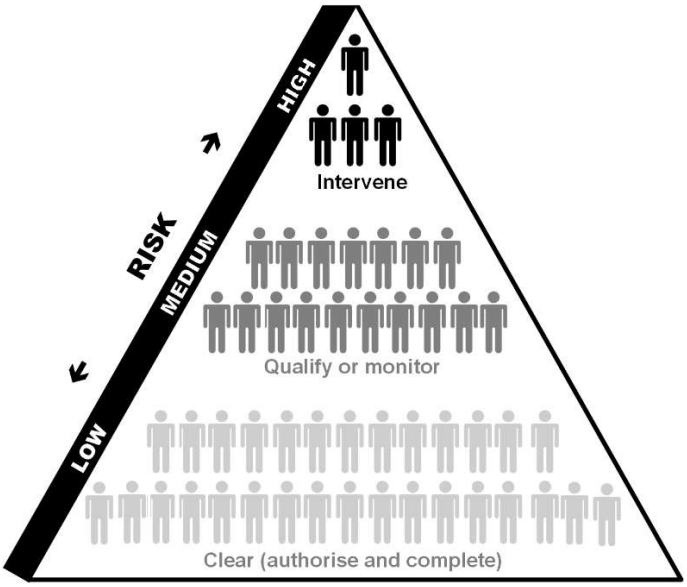
[83] Ibid. See also David Widdowson "Managing Risk in the Customs Context" in Luc De Wulf and Jose B Sokol *Customs Modernization Handbook* (World Bank, Washington DC, 2005) 91, at 92.

[84] For more information on the risk-assessment process used by New Zealand Customs, see Rebecca Foley and Bruce Northway "Managing Risk in Customs: Lessons from the New Zealand Customs Service" (2010) World Bank <openknowledge.worldbank.org>.

transactions to ensure the risk-assessment is sound. Ladley and Simmons describe this as the doctrine of "high assurance, light touch".[85]

The risk-management approach is illustrated in Figure 6.

**Figure 6. Border risk-management**




Customs administrations share information with other domestic agencies and foreign governments to enable better risk-management. Broader cooperation between government agencies to achieve shared outcomes is a priority in New Zealand.[86] The concept of shared outcomes is similarly used by foreign governments to achieve more efficient and effective use of resources.[87] In the customs context, intelligence is used to achieve shared security and compliance goals. In this regard, Walker states "It is an article of faith… that good intelligence is vital to defeating terrorism as well as being a currency more important than firepower".[88] Security intelligence-sharing has received

[85] Ladley and Simmons, above n 76, at 24.

[86] For example, see Bill Ryan and Derek Gill "Managing for Joint Outcomes" (2008) 4(3) Policy Quarterly 39, at 39. See also New Zealand State Services Commission and The Treasury *Performance Measurement: Advice and Examples on How to Develop Effective Frameworks* (Wellington, 2008), at 6.

[87] See generally *The Single Window Concept: Enhancing the Efficient Exchange of Information between Trade and Government* ECE/TRADE/324 (2003); Maurice Atkinson and Valerie Maxwell "Driving Performance in a Multi-Agency Partnership using Outcome Measures: A Case Study" (2007) 11(2) Measuring Business Excellence 12. See also Christine Ryan and Peter Walsh "Collaboration of Public Sector Agencies: Reporting and Accountability Challenges" (2004) 17(7) International Journal of Public Sector Management 621, at 621.

[88] Clive Walker *Terrorism and the Law* (Oxford University Press, Oxford, 2011), at 55; Prime Minister and the Secretary of State for the Home Department "Countering International Terrorism: The United Kingdom's

increased focus from governments since the Al Qaeda terrorist attacks in the United states on 11 September 2001 (the 9/11 terrorist attacks).[89] It has become commonplace in policy, media and expert circles to recognise the transnationalism of terrorism.[90]

Customs administrations exchange and use security intelligence in their shared responsibilities for border security, economic security and pandemic control.[91] Intelligence is used in risk-management processes to identify and exclude prohibited goods whilst allowing legitimate goods to pass unimpeded. Compliance costs and delays for legitimate traders are reduced through customs' use of intelligence, as interventions focus on those transactions deemed to be of high or moderate risk.[92]

Stepanova points out that intelligence cooperation is the most important form of international counter-terrorism cooperation but is still mainly confined to information-sharing. Joint counter-terrorism operations, such as the French-Spanish efforts to confront "Euskadi Ta Askatasuna" (ETA) are much less frequent.[93]

Presently, intelligence-sharing for customs purposes between New Zealand and other states is generally facilitated by bilateral agreements. The nature of each arrangement is unique. For example, New Zealand's arrangement with the United Kingdom includes four pages of provisions relating to the sharing and use of information.[94] In contrast, the cooperative arrangement between New Zealand and Korea is three pages in total and contains only seven bullet points relating to information-sharing and use.[95] Those terms

Strategy" (July 2006) United Kingdom Home Office <www.gov.uk>, at 16 and United Kingdom Chief of the General Staff *Operation Banner: An Analysis of Military Operations and Northern Ireland (Army Code 71842)* (Ministry of Defence, London, July 2006), at 8-4.

[89] Helen Fessenden "The Limits of Intelligence Reform" (2005) 84(6) Foreign Affairs 106, at 106.

[90] Ekaterina Stepanova "Terrorism and Antiterrorism" in Mary Kaldor and Iavor Rangelov (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 126, at 130.

[91] Ladley and Simmons, above n 76, at 7.

[92] WCO and UNCTAD, above n 77, at 2.

[93] Stepanova, above n 90, at 140.

[94] Cooperative Arrangement between Customs Authorities, New Zealand – United Kingdom (1996) (not deposited, provided to the author by the New Zealand Customs Service) (1996 New Zealand – United Kingdom Agreement).

[95] Cooperative Arrangement between Customs Administrations, New Zealand – South Korea (1992) (not deposited, provided to the author by the New Zealand Customs Service)(1992 New Zealand – Korea Agreement)(1992 New Zealand – South Korea Agreement).

differ from terms in other arrangements, such as between Japan and Canada and between Japan and Hong Kong.[96]

## *II The Information Needed for Trade Risk-Management*

This Part outlines at a general level the data that customs administrations collect and use for investigations and risk-assessments. This scope of data is included in the measures set out in Chapter Five and the legal framework described in Chapter Seven. Customs administrations use information from a variety of government, public domain and commercial databases.[97] It is not possible to discuss all the data used by customs administrations in great detail without revealing intelligence gathering and risk-assessment methodologies. Also, intelligence data requirements change as a result of the increasing use of computer technology to automate the supply chain.[98] Computerisation and the use of complex algorithms makes risk-management and intervention more sophisticated.[99] The scope of the intelligence data needed evolves over time as criminals also become more sophisticated and/or alter their targets and techniques.[100] Nonetheless, detailed analysis of specific intelligence data elements is not required for the development of the legal framework. It is recommended that the WCO Data Model, a standard for customs information, should be extended and should continue to evolve to include all the data needed for customs risk-management.[101]

Some of the information required for investigations and risk-assessments is already available in the WCO Data Model. The WCO Data Model version 3 began development

[96] Border Services Agency Mutual Assistance Agreement, Japan – Canada (2005) (not deposited, retrieved from www.customs.go.jp/english/cmaa) and Customs Co-Operation and Mutual Administrative Assistance Agreement, Japan – Hong Kong (2008) (not deposited, retrieved from www.customs.go.jp/english/cmaa).

[97] For example, see Rennie, above n 16, at 8.

[98] See UNECE "Trade Facilitation Implementation Guide: Customs Risk Management and Selectivity" (2015) United Nations Economic Commission for Europe <tfig.unece.org>; UNECE "Trade Facilitation Implementation Guide: Customs Automation" (2015) United Nations Economic Commission for Europe <tfig.unece.org> and Phil Williams "Organized Crime and Cybercrime: Synergies, Trends, and Responses" (2001) Computer Crime Research Centre <crime-research.org>. See also Martyn Dunne "New Zealand Customs Service: Changes over the Last Decade and into the Future" (2007) 1(1) World Customs Journal 41, at 46.

[99] Russell G Smith "Trends and Issues in Criminal Justice" (2004) Computer Crime Research Centre <crime-research.org>; *Paperless Trade in International Supply Chains: Enhancing Efficiency and Security* ECE/TRADE/351 (2008).

[100] Trend Micro Incorporated "Cybercriminals Reinvent Methods of Malicious Attacks" (7 July 2008) Help Net Security <www.net-security.org>. See also Ladley and Simmons, above n 76, at 28.

[101] "WCO Data Model", above n 34.

in June 2005 and is intended to aid the implementation of a single window system.[102] The data model is a standardised set of legally required data elements for not only customs' transactional needs but also partner agencies such as agriculture, health, environment and marine safety.[103] It contains data elements that can be grouped in nine classifications:[104]

1. Documentation references;
2. Dates, times, periods of time;
3. Parties, addresses, places, countries;
4. Clauses, conditions, terms, instructions;
5. Amounts, charges, percentages;
6. Measures, identifiers, quantities (other than monetary);
7. Goods and articles: descriptions and identifiers;
8. Transport methods and containers; and
9. Other data elements.

States that use the WCO Data Model can share this data with other states to facilitate trade transactions. This fixed format is essential for automated electronic communications. Presently, however, not all single window implementations use the same set of standards for information exchange. For example, the ASEAN states are sharing information in a format different to that prescribed by the WCO Data Model.[105]

The WCO Data Model is designed to allow traders to "lodge standardised information, mainly electronic, with a single entry-point to fulfil all import, export and transit related regulatory requirements".[106] It includes identifying and descriptive information about the entities involved in export and import transactions. Figure 7 illustrates some of the entities typically involved in these transactions.[107]

[102] Ibid.

[103] Ibid.

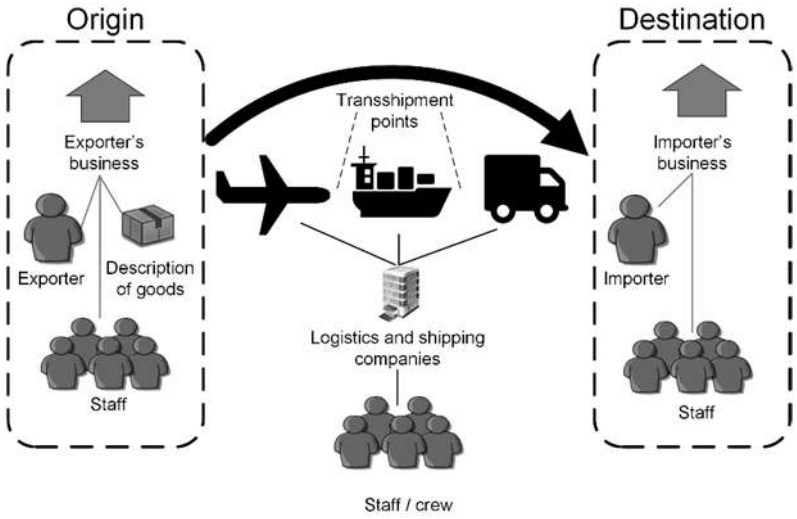
[104] WCO "WCO Data Model Single Window Data Harmonisation" (1 October 2014) World Customs Organisation <www.wcoomd.org>, para 6.3.

[105] SCCP, above n 55, at 109.

[106] "WCO Cross-Border Regulatory Agencies Customs Data Model: General Information" (2008) World Customs Organisation <www.wcoomd.org>, at 22.

[107] See also Truel, above n 77, at 9.

**Figure 7. Some entities involved in an import/export transaction**




An entity is a person, place, business, craft or goods item involved in the transaction. In the figure above, the entities shown to be involved in the transaction are:

1. The exporting business;
2. Staff at the exporting business;
3. The place of the exporting business;
4. The logistics and shipping companies;
5. Customs administrations and other government border agencies;
6. The logistics and shipping companies' staff and craft;
7. The importing business;
8. Staff at the importing business;
9. The place of the exporting business; and
10. The goods being transacted.

The information available in the WCO Data Model helps create an intelligence picture and risk profile for each entity. However, the intelligence value of the information available in the WCO Data Model is limited by its transactional focus. Each of the entities may be connected with intelligence information gained from other sources that informs the risk profile, or that creates connections with other entities that have a risk profile. For example, in respect of persons, a person may have a criminal record or criminal associations that increase the risk to customs of that person's border transaction. This could be, for example, a record of criminal convictions for the supply of prohibited drugs, or a current business association with known drug traffickers. A history of drug offences is a recognised risk indicator for drug-related and other crimes.[108]

[108] A M Gordon "Do Drug Offences Matter?" (1978) 2(6131) British Medical Journal 185, at 186.

Similarly, a place may also be connected with certain types of risk. For example, a place may be known as a common source of drugs or weapons.[109] A particular type of goods may also present risk.[110] For example, some types of traditional medicines frequently contain parts of endangered and internationally protected flora and fauna.[111] Trade of these goods may be restricted or prohibited by the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES).[112]

The scope of intelligence data needed by customs administrations to risk-assess these entities varies according to the situation. For example, in relation to the risk of drug crime, a customs administration will be interested in evidence of prior offending, among other things. In relation to the risk of endangered and internationally protected flora and fauna in traditional medicines, a customs administration will be interested in the line of business of the exporter or the importer and the history of prior imports.

Examples of the basic information that is required by customs risk-assessment systems include:[113]

1. Date of birth;
2. Mailing address;
3. Telephone number;
4. Social security number;
5. Email address;
6. Employer and employment relationships;
7. Associates – professional and personal;
8. Passport and numbers;
9. Driver licence state of issuance and number;
10. Description of the individual's physical characteristics; and
11. Firearms licence number.

[109] For example, see Richard Engel "Drugs, Weapons and Mexico" (21 October 2010) MSNBC <dailynightly.msnbc.msn.com>.

[110] Rennie, above n 16, at 8.

[111] Italian State Forest Corps "Operation Marco Polo: An Italian Investigation on the Illegal Trade in Asian Traditional Medicine" (10 February 2004) CITES Secretariat <cites.org>.

[112] Convention on International Trade in Endangered Species of Wild Fauna and Flora 993 UNTS 243 (1973).

[113] Frank Sisto "Privacy Impact Assessment for the Law Enforcement Information Database" (2008) US Department of Homeland Security <dhs.gov>, at 5, for the US Department of Homeland Security Law Enforcement Information database (Pathfinder) system. See also Council Decision 2015/219/EU Replacing the Annex on the SIRENE Manual for SIS II [2015] OJ L44/75, at s 2.11.3 for the European Union SIRENE II system; INTERPOL "INTERPOL's Rules on the Processing of Data III/IRPD/GA/2011(2016)" (2014) INTERPOL <www.interpol.int>, art 83 for INTERPOL requirements and WCO "SAFE Framework of Standards to Secure and Facilitate Global Trade" (June 2012) World Customs Organisation <www.wcoomd.org>, at Annex II for some of the data required by customs.

Similar types of personal information are described in the 1977 WCO Mutual Assistance Convention (the Nairobi Convention), which attempted to establish a framework for sharing customs intelligence.[114] The Nairobi Convention is discussed in more detail in Part III of Chapter Five.

The WCO Data Model does not contain information such as an individual's physical description. Intelligence like this can be useful for risk-management and investigation purposes. Intelligence material is often produced and shared in an unstructured or free-text format, such as a report.[115] The WCO Data Model, designed for developing a single window, uses only structured data elements comprising fields of fixed format for specific data types. It should be possible to add free-text data elements to extend the data model for intelligence purposes. The WCO Data Model would then be an appropriate vehicle for both trade transaction information and the intelligence information necessary to assess the risk posed by those trade transactions.

Other international standards exist for electronically exchanging trade transaction information, such as the Extensible Mark-up Language (XML), Electronic Data Interchange for Administration Commerce and Transport (EDIFACT), the United Nations Trade Data Elements Directory (UNTDED) and the WCO Unique Consignment Reference (UCR).[116] While some of these other standards can be used to define how information will be exchanged, the WCO Data Model is designed to provide harmonisation of what information is exchanged. Harmonisation of standards for both how and what information will be exchanged is essential to the implementation of an international single window.

The WCO Data Model defines the range and format of information that customs administrations collect and exchange for international trade transactions.[117] However, it does not include data elements specific to intelligence-sharing and a single window is not yet used as a vehicle for intelligence-sharing. Intelligence is a subset of information. The processes for sharing intelligence information and non-intelligence information can be the same. Trade transaction data and intelligence are both collections of structured and unstructured or free-text information. Both types of information can be exchanged using an agreed format such as the WCO data model.

---

[114] International Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offences (Nairobi Convention) UNTS 1226 I-19805 144 (opened for signing 9 June 1977, entered into force 21 May 1980), annex IX (9).

[115] For example, see Sisto, above n 113, at 3.

[116] APEC, above n 58, at 114 and "WCO Data Model", above n 34.

[117] "WCO Data Model", above n 34.

Intelligence can include qualitative information or subjective opinion and can therefore have varying reliability. This can create problems for data quality.[118] Accordingly, it would be prudent for the intelligence supplied through the legal framework to be accompanied by information that indicates the supplying party's assessment of the reliability of the information. The Admiralty System is one method that is used by intelligence analysts to articulate the accuracy of intelligence. The Admiralty System is used to grade the quality of intelligence by reliability of source and by credibility of the information.[119]

The WCO Data Model should be extended to include the data elements needed for sharing intelligence in support of the legal framework proposed here. The Admiralty System is not mandated in the proposed legal framework. However, if the WCO data model is extended in order to implement the legal framework, accuracy gradings from the Admiralty System or a similar system should be included within the model. That would enable customs officers to consider the quality of the intelligence they use when making risk management decisions.

### *III The National Security Role of Customs*

The role of customs administrations in the protection of the state's security interests is discussed in this Part. It provides more background to the reasons why some information would be exchanged through a single window system under the proposed legal framework and why some of that information, and its sources, must remain secret. Customs authorities rely on the broadest range of intelligence when making decisions about the border crossings of people, goods and craft.[120] These decisions are made on the basis of a risk-assessment. Intelligence used in the risk-assessment is drawn from the information a government collects. This can include, at a macro level, political and economic developments and information about specific places and events. At a micro level, this might include evidence or suspicion of criminal or terrorist associations and convictions, past travel movements, financial relationships, or suspicious or unwelcome behaviour. In New Zealand, the purpose of the customs decisions is to deny the entry of foreign people, goods or craft that pose a risk to the state's security, economy and society,

[118] Data quality is a privacy principle discussed in Chapter Four.

[119] For a discussion on the Admiralty System see Don McDowell *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users* (Scarecrow Press, Plymouth, 2008), at 209 and John Joseph and Jeff Corkill "Information Evaluation: How one Group of Intelligence Analysts go about the Task " (4th Australian Security and Intelligence Conference, Edith Cowan University, 5 -7 December, 2011), at 99.

[120] In customs, the term craft is used to mean vehicles and sea-going vessels.

whilst facilitating and promoting legitimate trade. The New Zealand Customs Service's role includes a general responsibility in respect of security:[121]

> Customs plays an active role in the international customs community, ensuring that there is active representation of New Zealand's interests in international customs policy, trade and security interests, and law enforcement relationships to deliver on our functions by being …. able to gather and use information and intelligence from both traditional and non-traditional partners to enable targeted upstream disruption, with offshore partners willing to act on our behalf to prevent harm reaching New Zealand's borders.

One meaning of security is safety or, as Fiona Robinson argues, being free of care: [122]

> This is the sense in which it was used by those who formulated the original version of human security. For them, calling it a security issue meant that it was important…. The second meaning of security is the identification with security services (the police, the military, intelligence services, etc.)…. But it is the third meaning of security that preoccupied the critics of human security. This is the understanding that security is having to do with a supreme emergency which is intrinsically linked to sovereign power.

In this sense it is the act of labelling an issue as a security issue that removes it from the realm of normal day-to-day administration, casting it as an "existential threat" and "justifying extreme measures".[123]

The New Zealand Customs Service's role in security and intelligence is supported with enabling legislation. Section 38B of the Customs and Excise Act 1996 allows the organisation to access information on border-crossing goods, persons and craft that may be related to border security, to the enforcement of other New Zealand laws, or to more general threats to the health and safety of the New Zealand public.

While the threat used to be narrowly defined, and there was a clear idea of a "national Other" as being a person from outside one's national boundaries, a look into national security strategies shows that the "against what" has broadened significantly. [124] The terrorist threat now requires a state to treat others as both potential friend and foe because

---

[121] New Zealand Customs Service "Statement of Intent 2017-2021" (2017) New Zealand Customs Service <www.customs.govt.nz>, at 7. There is no express statutory provision to this effect.

[122] Fiona Robinson *The Ethics of Care: A Feminist Approach to Human Security* (Temple University Press, Philadelphia PA, 2011), at 42.

[123] Mary Kaldor "Human Security" in Mary Kaldor and Iavor Rangelov (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 85, at 97-98.

[124] Sabine Selchow "Security Policy and Global Risks" in Mary Kaldor and Iavor Rangelov (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 68, at 70.

the nature of terrorism is "intimate, local and indigenous".[125] Walker and Rehman explain:[126]

> The main terrorist threat is no longer from [the] archetypal outsider embodied by the convenient figure of the now deceased Osama bin Laden – depicted as an alien, uncivilised cave dweller who imports terrorism from foreign lands.

In this regard, the United Kingdom national security strategy states: [127]

> The world is changing rapidly and fundamentally. We are seeing long-term shifts in the balance of global economic and military power, increasing competition between states, and the emergence of more powerful non-state actors. We are increasingly likely to have to deal with unexpected developments.

The role of the New Zealand Customs Service in contributing to security and intelligence gathering is described by the Department of the Prime Minister and Cabinet, which set out the national security goals as:[128]

1. Preserving sovereignty and territorial integrity: Protecting the physical security of citizens, and exercising control over territory consistent with national sovereignty.
2. Protecting lines of communication: These are both physical and virtual and allow New Zealand to communicate, trade and engage globally.
3. Strengthening international order to promote security: Contributing to the development of a rules-based international system, and engaging in targeted interventions offshore to protect New Zealand's interests.
4. Sustaining economic prosperity: Maintaining and advancing the economic well-being of individuals, families, businesses and communities.

---

[125] Clive Walker and Javaid Rehman "'Prevent' Responses to Jihadi Extremism" in Victor V RamRaj, Michael Hor, Kent Roach, and George Williams *Global Anti-Terrorism Law and Policy* (2nd ed, Cambridge University Press, Cambridge UK, 2012) 242, at 247.

[126] At 247.

[127] UK Government *National Security Strategy and Strategic Defence and Security Review 2015* (Her Majesty's Stationery Office, London, 2015), at 15. This security strategy remains in force and progress has been reported in UK Government *National Security Strategy and Strategic Defence and Security Review 2015: First Annual Report 2016* (Her Majesty's Stationery Office, London, 2016).

[128] Department of the Prime Minister and Cabinet "National Security System" (2011) Department of the Prime Minister and Cabinet <www.dpmc.govt.nz>. See also the description of national security impact in the information security classifications set out in the current government security manual, which is the Department of the Prime Minister and Cabinet "Security in the Government Sector" (2002) Government Communications Security Bureau <www.gcsb.govt.nz>.

5. Maintaining democratic institutions and national values: Preventing activities aimed at undermining or overturning government institutions, principles and values that underpin New Zealand society.
6. Ensuring public safety: Providing for, and mitigating risks to, the safety of citizens and communities (all hazards and threats, whether natural or man-made).
7. Protecting the natural environment: Contributing to the preservation and stewardship of New Zealand's natural and physical environment.

New Zealand participates in intelligence-sharing arrangements with partner states. It is "firmly committed" to the concept of collective security because of its reliance as a small economy on the well-being of its trading partners.[129] The proposed legal framework supports collective security by improving intelligence-sharing between customs administrations.

## *IV State National Security and Law Enforcement Objectives*

This Part builds on the ideas introduced in Part III above, by describing the security and law enforcement objectives the state seeks to achieve with the intelligence information it collects and shares. This Part does not provide an in-depth analysis or provide judgements on the various concepts of national security. It explains that the terms security and national security can be broadly interpreted to include objectives other than physical safety, sovereignty, or political stability. Other interpretations include protecting economic wellbeing and obtaining economic advantage. The various interpretations of security might conflict with the values of some members of the public and affect their confidence in the purposes of the proposed legal framework. The validity or morality of the various interpretations are not examined here, nor are normative statements offered on the definition of security. The thesis aims to provide a practical means to share intelligence and it does not set out to examine or challenge the role and responsibilities of customs administrations.

Barkin and Cronin put forward a view that "a realist may argue sovereignty is based less on a set of principles than on the ability of a political group to establish control over a territory and defend it from external attack".[130] Intelligence collection and sharing is fundamental to this ability of governments to protect their borders and enforce their laws. This is recognised by James Rule, who argues:[131]

[129] David Lange "New Zealand's Security Policy" (Summer 1985) 63(5) Foreign Affairs 1009, at 1009.

[130] J Samuel Barkin and Bruce Cronin "The State and the Nation: Changing Norms and the Rules of Sovereignty in International Relations" (1994) 48(1) International Organisation 107, at 110.

[131] James Rule *Privacy in Peril: How we are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Oxford University Press, New York, 2007), at 40.

> What governments can know about their people – about their family situations, their wealth or lack of it, their political inclinations, or indeed their whereabouts – has everything to do with what laws can be upheld, what revenues can be extracted and what forms of compliance will be forthcoming from the governed.

The need for intelligence-sharing for border security escalated after the 9/11 terrorist attacks. The security role of many government agencies changed as a result of those attacks. For example, seven months after the attacks, the United States Attorney-General, John Ashcroft, changed the investigative guidelines of the Federal Bureau of Investigation (FBI) to "prevention above all else".[132] A similar change occurred in the security focus of border agencies. This was because poor border control allowed the movement of members of Al Qaeda, Jemaah Islamiyah and other terrorist organisations to cross international borders before major terrorist attacks.[133]

As discussed in Part I, the analysis of intelligence is necessary for the effective risk-management of trade which is non-compliant with customs law. In New Zealand, the role of customs extends beyond the enforcement of trade law. It includes enforcing other laws and protecting the health and safety of the public. The Customs and Excise Act 1996 states:[134]

> The Customs may collect, use, or disclose the information for any of the following purposes (and, in the case of personal information, despite anything in information privacy principles 2, 3, 10, or 11 of the Privacy Act 1993):
>
> (a) exercising or performing a power, function, or duty under this Act:
>
> (b) the prevention, detection, investigation, prosecution, and punishment of offences that are, or that if committed in New Zealand would be,–
>
> (i) customs offences of any kind; or
>
> (ii) other offences punishable by imprisonment:
>
> (c) the processing of international passengers at the border by public authorities:
>
> (d) the protection of border security:
>
> (e) the protection of the health and safety of members of the public.

[132] Athan Theoharis *The Quest for Absolute Security: The Failed Relations Among US Intelligence Agencies* (Ivan R Dee, Chicago, 2007), at 3.

[133] Paul Smith (ed) *Terrorism and Violence in Southeast Asia: Transnational Challenges to States and Regional Stability* (East Gate, New York, 2005), at xiii.

[134] Section 282A. This section was inserted on 2 July 2004, by section 43 of the Customs and Excise Amendment Act 2004 (New Zealand).

Section 281 of the Customs and Excise Act 1996 also empowers the customs administration to share information for "the enforcement of a law imposing a pecuniary penalty" and "the protection of public revenue".[135] A "pecuniary penalty" could include offences such as parking fines or unpaid dog licencing which have no relationship to border or trade security. Section 281 could also be used to disclose information that could be used to restrict the movements of anti-free trade or anti-globalisation protestors.[136] Such an outcome could be viewed as a political rather than a national security, border or trade security objective.

It is relevant to note that the Government Communications Security Bureau (GCSB) has a specialist trade team which pre-dated recent allegations that the government was spying on the rivals of New Zealand's candidate for the position of WTO Director-General.[137] The existence of such a team reinforces the notion that New Zealand is actively seeking intelligence to promote or secure its economic interests. Activity like this would sit well with Robinson's broader definition of security to include all aspects of "safety" such as economic well-being.[138]

Customs has authority to collect, use and share information for security purposes. The New Zealand Customs and Excise Act 1996 uses the catch-all phrases "border security" and "security" which are not defined.[139]

The objectives of the GCSB and the New Zealand Security Intelligence Service (NZSIS) are equally wide-ranging in this respect. The Intelligence and Security Act 2017 states:[140]

> The principal objectives of the intelligence and security agencies are to contribute to—
> (a) the protection of New Zealand's national security; and
> (b) the international relations and well-being of New Zealand; and
> (c) the economic well-being of New Zealand.

---

[135] Section 281, paragraphs (1)(d) and (1)(e).

[136] See also Mark Pythian "The British Experience with Intelligence Accountability" (2007) 22(1) Intelligence and Security 75, at 76, in which he discusses the move towards greater accountability of security and intelligence agencies in the 1970s and 1980s as the result of a widespread belief that the agencies were "interfering with legitimate political dissent".

[137] David Fisher "GCSB spies Monitored Diplomats in Line for World Trade Organisation job" *The New Zealand Herald* (online edition, Auckland, 23 March 2015) and Jane Kelsey "Is the GCSB 'Trade Team' Spying on NZ's TPPA 'Partners'?" (24 March 2015) Scoop Media <www.scoop.co.nz>.

[138] Robinson, above n 122, at 7.

[139] "Border security" appears in the Customs and Excise Act 1996 12 times in five sections starting with s 38B, but not as a definition in the Interpretation at s 2. The Act uses the term "security" in respect of national security at s 38N and again without definition in the Interpretation at s 2.

[140] Section 9.

This definition allows a broad interpretation that could include the legitimate trading activity of businesses or individuals. Security analyst Buchanan says in respect of intelligence and New Zealand legislation that "the government enjoys having that grey area left somewhat ambiguous because it gives room for manoeuvre".[141] This ambiguity could allow government agencies to use the powers vested in them to treat protests which might be deemed lawful in New Zealand as threats to "economic well-being", for example: [142]

> The Occupy Movement, as it has come to be called, boasts movements in more than 1500 cities around the world …. the Occupy protests could be seen as a threat to the financial stability of the United States, which, given its place in the global financial system, might even be a threat to the global economic system as a whole. It might not be a military threat, but it is certainly a threat of some kind to the "security" of the state.

This kind of "totalitarian" intrusion by the state into lawful protest and political opposition occurred in the 1970s, was investigated, and was widely reported in the United States.[143]

The concept of economic security also creates mistrust, according to a 2007 report of the European Commission for Democracy, because:[144]

> Allowing the collection of signals intelligence for "the economic well-being of the nation" gives rise to the suspicion that signals intelligence is being used for purposes of economic espionage, to win commercial advantages for companies incorporated in a state's own jurisdiction in public procurement or other areas

For customs' purposes in respect of its use of the proposed legal framework, the protection of economic security as an element of border security might be claimed in defence of disclosures of personal information. The trade-off of the rights of its citizens against sovereign security, law enforcement or economic interests could be enabled by

---

[141] Paul Buchanan "Analyst Says NZ Needs More Oversight of Intelligence Agencies" (22 May 2013) Morning Report, Radio New Zealand <www.radionz.co.nz>.

[142] David Mutimer "Security and Social Critique" in Mary Kaldor and Iavor Rangelow (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 31, at 38.

[143] *Intelligence Activities and the Rights of Americans: Book II - Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities* 94th Congress 2nd Session, S Rept 90-755 (1976), at 3 and Glenn Greenwald *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books, New York, 2014), at 184.

[144] European Commission for Democracy through Law (Venice Commission) Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies [2013] CDL-AD(2015)006, at [77].

the broad powers granted to customs through legislation, namely s 281 of the Customs and Excise Act 1996. That section provides customs with the authority to disclose information "to an overseas agency, body or person" for a range of purposes. Those purposes may be for New Zealand's benefit or for the benefit of that overseas agency, body or person. The purposes are set out in the legislation. Valid purposes for sharing information include the enforcement of a law imposing a pecuniary penalty, or the protection of public revenue.[145]

Surveillance of economic targets is a specific objective of New Zealand, Canadian and United Kingdom law and is enabled by more generalised clauses in Australian and United States laws.[146] Gearan reports that the Obama administration in the United States asserted to other states that, like the USA, every other country spies.[147] In light of these facts, Roughan argues economic spying is justified because "a free and fair global trading environment is not a universal goal of governments, though nearly all pay lip service to it".[148] A state will be reluctant to participate in an intelligence-sharing arrangement that enables it to be the subject of economic spying. States should be able to withhold intelligence when sharing it could compromise the interests of the state. Many existing agreements and Memoranda of Understanding, discussed in Chapter Five, enable this voluntary approach to cooperation. However, some of these agreements, notably the Memoranda of Understanding, are not easily accessible and have been made without reference to parliamentary process or other mechanisms that would allow democratic debate. The absence of public scrutiny and debate is likely to hinder public confidence in the intelligence-sharing arrangements. Accordingly, the proposed legal framework should enable intelligence to be shared voluntarily between states, but not compelled.

The role of secrecy in national security and law enforcement is discussed in the next Part.

## *V The Need for Secrecy*

In the course of maintaining security, law and order, there is a duty in regard to protecting the confidentiality of intelligence. This can include secrecy for the existence of the

[145] Section 281(1).

[146] Intelligence Services Act 1994 (MI5 and MI6 Act) (United Kingdom), s 1(2)(c); Canadian Security Intelligence Service Act 1985 (Canada SIS Act) (Canada), s 16(1)(b)(iii); 50 USC § 1802 (United States), at (a)(1) and Intelligence Services Act 2001 (ASIS Act) (Australia), s 6(1)(a) and s 7(a).

[147] Anne Gearan "Spying on France Causes Diplomatic Headache" (22 October 2013) Fairfax Media <www.stuff.co.nz> and Anne Gearan "Report that NSA Collected French Phone Records Causing Diplomatic Headache for US" *The Washington Post* (online ed, Washington DC, 23 October 2013).

[148] John Roughan "Spying on WTO Justified by Economic Ambitions" *The New Zealand Herald* (online edition, Auckland, 28 March 2015).

intelligence, keeping the methods used to collect intelligence secret and protecting the source of the intelligence.

The proposed legal framework provides a practical solution for automating existing exchanges of intelligence by customs administrations and at the same time provides some transparency to the treatment of human rights and privacy, even though the intelligence itself must remain secret. The protection of human rights and privacy in the treatment of secret intelligence are a good and an end in themselves. Transparency of the controls that support this protection in the legal framework would enable democratic debate, which should engender increased public confidence in the system.

The need for secrecy is enshrined in most intelligence-sharing agreements as a confidentiality clause.[149] Disclosure of the source and content of intelligence can reveal sensitive methodologies to criminals and through this enable criminals to put countermeasures in place. It can also place the source of intelligence under the threat of physical harm or death. These factors weaken governments' ability to combat crime. The United States National Security Council recognised this in its Intelligence Directive No. 11, which states:[150]

> The Departments and Agencies of the Government engaged in intelligence activities shall take steps to prevent unauthorised disclosure of information on United States intelligence sources and methods …. The delimiting phrase "intelligence sources and methods" includes information ostensibly overt which requires security protection because of its specific means of procurement or specific place of procurement, revelation of which would endanger intelligence sources and methods …

The National Security Council's responsibility is "the integration of domestic, foreign, and military policies relating to the national security".[151] However, these same concerns apply to all the intelligence used by customs. Part IV discussed the national security remit of customs administrations. This includes the movement of weapons and other goods that may support terrorism, but also includes other transnational crimes such as people smuggling, illicit drugs, child sex crimes, copyright infringement, movement of the proceeds of crime and government revenue (tax, duty and excise) fraud.

For customs' purposes in respect of the proposed legal framework, maintenance of the law, maintenance of information-sharing relationships and national security or border

[149] For examples, see Stabilisation and Association Agreement, European Union – Albania OJ L107/165 (2009), art 10 of Protocol 6 and Cooperative Arrangement between Customs Authorities, Japan – United States of America (1997) (not deposited, retrieved from www.customs.go.jp/english/cmaa), art 9(3).

[150] National Security Council "National Security Council Intelligence Directive No. 11: Security of Information on Intelligence Sources and Methods" (1950) Central Intelligence Agency <foia.cia.gov>.

[151] 50 USC § 402.

security might be claimed by the state in defence of disclosures of information that would otherwise remain secret. In its desire to protect its own citizens and economic interests and to intervene on behalf of others, a customs administration could be motivated to set aside the rights and freedoms of certain individuals in the pursuit of better outcomes for a community or society as a whole.[152] This admittedly utilitarian approach to human rights is not universally accepted because:[153]

> … utilitarianism, in principle, permits the interests of the majority to over-ride the rights of minorities …. The charge is that utilitarians assign no independent weight to justice.

By way of example, human rights were arguably traded-off against sovereign interests during the Second World War, as evidenced by the exceptional English case of *Liversidge v Anderson*.[154] The power of unilateral decision making was conferred on the Secretary of State for Home Affairs (the Home Secretary), Sir John Anderson, by the Defence (General) Regulations 1939. Under these regulations, the Home Secretary could imprison Robert Liversidge on the grounds that there was a reasonable cause to believe that Liversidge had hostile associations.[155]

A different approach was taken in the later case of *Nakkuda Ali v M F de S Jayaratne*, in 1950. *Nakkuda Ali* was a step towards the transparent use of state powers when limiting or infringing on individual rights.[156] In this case, the Privy Council supported Lord Atkin's dissenting views.[157] The Controller of Textiles had cancelled a textile dealer's licence. Regulatory power enabled the Controller of Textiles to cancel licences if "the Controller has reasonable grounds to believe that any dealer is unfit to be allowed to continue as a dealer".[158] The Privy Council held that there must in fact exist reasonable grounds, known to the Controller, before he could validly exercise the power of cancellation. It decided that the Controller's decisions should be subject to judicial review and the words of the regulation requiring "reasonable grounds" meant that those

[152] Simon McKay *Covert Policing: Law and Practice* (Oxford University Press, Oxford, 2011), at 49 para 2.116.

[153] Tom L Beauchamp and James F Childress *Principles of Biomedical Ethics* (5th ed, Oxford University Press, New York, 2001), at 347.

[154] *Liversidge v Anderson* [1941] UKHL 1, [1941] 3 All ER 338, [1942] AC 206.

[155] Liversidge claimed that he should not have been imprisoned, but his claim was unsuccessful.

[156] *Nakkuda Ali v M F de S Jayaratne* [1950] UKPC 17, [1951] AC 66, 66 TLR (Pt 2) 214, (1950) 10 CR 421.

[157] Ibid.

[158] Defence (Control of Textiles) Regulations 1945 (Ceylon), regulation 62.

grounds must be evident for the Controller to legitimately make such a decision.[159]

In addition to self-defence, there may sometimes be an opportunity created by the enabling legislation of customs and intelligence agencies to seek economic advantage for the parent state.[160] It would be problematic if a state was motivated to manipulate an intelligence-sharing system to extend its access to resources and/or its political power. For example, a state could introduce information into the system to discredit competitor states and gain advantage in trade negotiations. Sovereign self-interest, the motivation for such manipulation, was recognised in the 16th century by Machiavelli who wrote:[161]

> Hence it is necessary for a prince who wishes to maintain his position to learn how not to be good, and to use this knowledge or not use it according to necessity.

The secret use of intelligence and setting aside an individual's rights for a sovereign purpose can erode public confidence in government intelligence-sharing. The legal framework proposed here does not attempt to constrain the role of customs administrations set out in domestic legislation. Instead, it brings transparency to the way information is shared for those purposes. Transparency of intelligence-sharing processes can help to protect or restore public confidence. That is the subject of the next Part.

---

[159] *Nakkuda Ali v M F de S Jayaratne*, above n 156. In another test of reasonable grounds in an import context, Judge Royce found in *Dulcie Holdings Ltd v New Zealand Customs Service* [1997] DCR 1077, at [1096], that New Zealand Customs' seizure of goods satisfied the test as set out in s 226(1) of the Customs and Excise Act 1996 that a Customs officer had "a reasonable cause to suspect" the goods should be forfeited under s 225 of the Act. Customs did not need to meet the standard of proof for "a reasonable cause to believe". In contrast, in *Bathurst Developments Ltd v New Zealand Customs Service* [1998] DCR 300, Judge Willy found that 9 of 10 vehicles should no longer be detained by Customs, as it had not satisfied the standard of proof for a "reasonable cause for the seizure, or the continued detention" as set out in s 231(1)(a) of the Customs and Excise Act 1996. Note that this test for continued detention has a higher bar than a "reasonable cause to suspect", as applied in *Dulcie* for Customs' initial seizure of goods. In a further test of reasonable grounds, this time involving secret information and the detention of a person, rather than the seizure of goods, the case of *Attorney-General v Ahmed Zaoui* SC CIV 19/2004 [2005] NZSC 38 addressed the question of whether there existed reasonable grounds for regarding Zaoui as a danger to the security of New Zealand under s 114C(6) of the Immigration Act 1987. Zaoui's detention raised a number of legal questions relating to the nature and duration of his detention and the secrecy of the information the Director of Security used to issue a certificate relating to him, meaning the information could not be easily challenged by Zaoui. The detention of Zaoui ended when the Director of Security withdrew the certificate that had been issued.

[160] For example, Intelligence and Security Act 2017 (New Zealand); Intelligence Services Act 1994 (MI5 and MI6 Act) (United Kingdom); Canadian Security Intelligence Service Act 1985 (Canada SIS Act) (Canada); 50 USC § 1802 (United States) and Intelligence Services Act 2001 (ASIS Act) (Australia).

[161] Niccolò di Bernardo dei Machiavelli "The Prince" in Peter and Mark Musa (eds) Bondanella *The Portable Machiavelli* (Penguin, Middlesex, 1979) 77, at 127.

## *VI Transparency and Public Confidence*

This Part provides the reasoning for making the legal framework for customs intelligence-sharing through a single window system, and its inherent controls for the treatment of human rights and privacy, subject to public scrutiny and debate. It is accepted as self-evident that this transparency will improve public confidence, just as a lack of knowledge generally increases uncertainty and more knowledge generally reduces doubt. The extent to which public confidence might be improved is not examined in-depth, predicted, or tested. It could be established through further empirical research, before and after the implementation of the legal framework.

Secret dealings by the state undermine the public's ability to participate in democracy by not fully informing them of the government's intentions and actions.[162] A state must have the confidence of its public to participate in the legal framework proposed here because, as Sutherland said: [163]

> The government, which has been organised to put the will of the Nation into operation, must go forward in aid of it …. The plenary power to determine all questions of government without accountability to any one – is in the people and nowhere else.

Sutherland's argument is that a democratic and representative government is not motivated to act against the will of its people, because doing so could bring about its own downfall. Even so, states work in secrecy to overcome threats to security and other crimes because to do otherwise would forewarn miscreants. It is that secrecy that creates opportunities for abuses of human rights. For example, the New Zealand news media has reported on public distress that data from a neonatal heel prick blood test, the Guthrie test, was stored indefinitely and was being used surreptitiously by the police for DNA analysis in homicide cases.[164] One parent was reported as feeling betrayed that a heel prick blood sample from her missing daughter had been used by police without her knowledge or consent. It has been reported that the Ministry of Health carefully considers "police guidelines", the circumstances and the wider public interest in law enforcement

[162] Frederick A Schwarz *Democracy in the Dark: The Seduction of Government Secrecy* (The New Press, New York, 2015), at 12.

[163] George Sutherland *Constitutional Power and World Affairs* (Columbia University Press, New York, 1918), at 2 and 482.

[164] Bevan Hurley, Sam Sherwood and Michael Hayward "Parents upset at police access to blood samples taken from babies" (15 October 2017) Fairfax Media <www.stuff.co.nz>. The Privacy Commissioner had previously identified matters of concern relating to the rules around storing and subsequent use of Guthrie Tests and had made recommendations, which had not been implemented by October 2017 in Privacy Commissioner "Guthrie Tests: A Report by the Privacy Commissioner following his Inquiry into the Collection, Retention, Use and Release of Newborn Metabolic Screening Test Samples, Pursuant to Section 13(1)(m) of the Privacy Act 1993" (September 2003) Office of the Privacy Commissioner <www.privacy.org.nz>, at 12 para 9.7.

and public safety before releasing heel prick information.[165] This approach allows access to private medical records without consent, a court order or a search warrant being obtained by the police. It requires the Ministry of Health to decide whether the release of the information is appropriate – a decision that the courts would make in other circumstances.

Loader and Walker note that "giving primacy to … 'expertise' is bound up with the vices of the state tradition".[166] In the United Kingdom this primacy is reflected in a degree of independence for the directors of the intelligence services.[167] The Minister in charge does not have day-to-day responsibility for the operation of the services, except for operations where a Ministerial warrant is required.[168] A Parliamentary select committee exists to oversee the administration of the intelligence services, but operational information of "a sensitive nature" is withheld from the committee.[169] Overall, intelligence accountability in the United Kingdom has been limited and it is a bureaucratic formality rather than substantive oversight.[170]

It has been also argued that government secrecy is "more dangerous to democracy than the practices they conceal".[171] Secrecy applies not just to information, as claimed by Maret, but also to information processing.[172] In contrast to the methods for *gathering* intelligence, the rules for sharing intelligence can and should bear scrutiny.

This is because secrecy erodes public trust and confidence in the government. In 1970, United States Congressman Conable declared "secrecy undermines the democratic

[165] Ibid, and Chris Barton "Dilemma of the life-saving cards" *New Zealand Herald* (online edition, Auckland, 8 May 2009).

[166] Ian Loader and Neil Walker *Civilizing Security* (Cambridge University Press, Cambridge, 2007), at 200.

[167] "Accountability of Security and Intelligence in the United Kingdom" in Hans Born, Lock K Johnson and Ian Leigh *Who's Watching the Spies: Establishing Intelligence Service Accountability* (Potomac Books, Dulles VA, 2005) 79, at 84 and 85.

[168] Ibid.

[169] At 88.

[170] Jon Moran and Clive Walker "Intelligence Powers and Accountability in the U.K." in Zachary K Goldman and Samuel J Rascoff (eds) *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (Oxford University Press, New York, 2016) 289, at 290.

[171] J William Fulbright "The High Cost of Secrecy" (1971) 39(9) The Progressive American Review of Public Administration 16.

[172] Susan Maret (ed) *Government Secrecy* (Emerald Group Publishing, Bingley, UK, 2011), in the introduction at xvii.

process and saps public confidence in the house".[173] The United Kingdom Intelligence Select Committee later said:[174]

> It is vital that public confidence is maintained …. [It] can be very fragile. That is the inevitable consequence of [the intelligence and security services] operating within the 'ring of secrecy', which prevents a more balanced public view of their activities and their value.

Edward Snowden's leak of 58,000 United States National Security Agency (NSA) documents exposed some of the previously secret collection and use of intelligence, including the data-mining of swathes of information collected about individuals as a form of surveillance.[175] The leak reduced public confidence in governments that were seen to be cooperating with the NSA and in New Zealand it led to public outcry over the legislation that empowered the GCSB, an intelligence agency.[176]

Public protests against the effect that secrecy has on the democratic process are evident in the media reports of the Trans Pacific Partnership (TPP) negotiation that was underway in 2015.[177] The TPP negotiations, announced at the APEC Trade Ministers Meeting in June 2005, evolved from an earlier preferential trade agreement known as the "Pacific Four" (P4).[178] The national security classification of the draft TPP agreement in the United States meant that it would "remain secret until long after meaningful public

---

[173] Andrew J Glass "Congressional Report/Legislative Reform Effort Builds New Alliances Among House Members" (1970) 2 National Journal 1607. See also Paul J Quirk and Joseph Hinchcliffe "The Rising Hegemony of Mass Opinion" in David Brian Robertson (ed) *Loss of Confidence: Politics and Policy in the 1970s* (Pennsylvannia State Press, University Park PA, 2010) 19, at 29.

[174] United Kingdom Intelligence and Security Committee *Annual Report 1997-1998* (Her Majesty's Stationery Office, London, 1998), in the Foreword.

[175] David Lyon *Surveillance after Snowden* (Polity, Cambridge, UK, 2015), at 17, 79 and 81.

[176] Robert G Patman and Laura Southgate "National Security and Surveillance: The Public Impact of the GCSB Amendment Bill and the Snowden Revelations in New Zealand" (2016) 31(6) Intelligence and National Security 871, at 875 and 876. The Government Communications Security Bureau Act 2003 (GCSB Act) was repealed in 2017 and replaced by the Intelligence and Security Act 2017.

[177] For example, see Eric Bradner "How Secretive is the Trans-Pacific Partnership?" (12 June 2015) CNN Politics <Edition.cnn.com>; Eileen Goodwin "TPP 'Cold War Taking Place By Proxy'" *Otago Daily Times* (online edition, Dunedin, 29 June 2015); Marjorie Arons-Barron "Secrecy tips the case of the Trans-Pacific Partnership" *Milford Daily News* (online edition, Milford MA, 5 June 2015); Susan Davis "Senate Panel Approves 'Fast Track' Trade Bill" *USA Today* (online edition, McLean VA, 22 April 2015); Mike Blanchfield "75 Percent of Canadians Unaware of TPP Negotiations: Poll" (17 June 2015) CTV News <www.ctvnews.ca> and Jon Schwarz "You can't read the TPP and you can't find out who in Congress has" (14 June 2014) The Intercept <firstlook.org>.

[178] C L Lim, Deborah K Elms and Patrick Low *The Trans-Pacific Partnership: A Quest for a Twenty-first Century Trade Agreement* (Cambridge University Press, New York, 2012), at 21.

debate is possible".[179] It was argued that the intrigue surrounding the trade negotiations created "a funnel where powerful interests congregate, absent the checks, balances and necessary hurdles of the democratic process".[180] The fact that the details were kept secret from the United States Congress was reported to be a cause of reluctance by some members of Congress to support the overall trade deal.[181] The United States had withdrawn from the TPP and the future of the agreement was uncertain until a new negotiation, excluding the United States, was announced following the APEC meeting at Vietnam in November 2017.[182]

The need for secrecy presents a paradox for governments that are required to operate secretly for law enforcement and national security reasons, because it is necessary at the same time to maintain the confidence of the electorate.[183] The proposed legal framework addresses this issue. It does not involve the creation of a centralised database for data-mining, which was a subject of Snowden's disclosures. However, it does involve the sharing of secret intelligence. It aims to improve public confidence in the processes that customs administrations use for sharing secret information. It will provide reassurance that effective controls exist to protect information from unauthorised disclosure and from being used for purposes that are not clear and previously agreed.

## *VII Factors Influencing Intelligence Cooperation*

This Part explains that an effective legal framework, even though it meets all the practical requirements for sharing intelligence through a single window system, is not enough on its own to enable intelligence-sharing between states. There are specific factors that influence the creation of new arrangements for intelligence cooperation. Intelligence work in general can create distance between the public and law enforcement agencies.[184] To address the risk of eroding public trust in the context of police intelligence processes,

---

[179] Margot E Kaminski "Don't Keep the Trans-Pacific Partnership Talks Secret" *The New York Times* (online ed, New York, 14 April 2015), at A23.

[180] Ibid.

[181] Bob Kinzel "Despite Welch's Vote, Trans-Pacific Trade Approved By Slim Margin In US House" (12 June 2015) Vermont Public Radio <digital.vpr.net>. On 23 January 2017, President Trump issued a presidential Memorandum ordering the withdrawal of the United States from the Trans-Pacific Partnership Negotiations and Agreement. See 82 FR 8497 Presidential Memorandum Regarding Withdrawal of the United States from the Trans-Pacific Partnership Negotiations and Agreement, 23 January 2017 (United States).

[182] Ministry of Foreign Affairs and Trade "Trans-Pacific Partnership" (2017) Ministry of Foreign Affairs and Trade <www.tpp.mfat.govt.nz> and Craig McCulloch "Exporters Welcome Revamped TPP, Critics have Doubts" (13 November 2017) Radio New Zealand <www.rnz.co.nz>.

[183] Michael P Colaresi *Democracy Declassified: The Secrecy Dilemma in National Security* (Oxford University Press, New York, 2014), at 101.

[184] Jerry Ratcliffe *Intelligence-led Policing* (Willan Publishing, Devon UK, 2008), at 222.

Porter argued that it is important to "…put the protection of privacy and civil liberties up front when implementing an intelligence-led policing approach".[185] This is also true for implementing customs intelligence processes and is the reason for the focus on the treatment of human rights and privacy in the proposed legal framework.

Tuzuner's model for considering the factors influencing intelligence cooperation identifies other factors and categorises them as either threat-based or independence-based.[186] The specific threat-based factor that Tuzuner examined was terrorism. However, non-terrorist transnational crime is also threat-based. Consideration of national security issues, including terrorism, has merged with criminal intelligence analysis. This enables security threats to be considered alongside other transnational crime in a more holistic approach to detecting and preventing crime.[187] Guymon argues that bilateral law enforcement cooperation is no longer sufficient to address the rising impact of transnational crime, reinforcing the need for a multilateral approach.[188]

These factors were discussed when feedback was sought from a sample of New Zealand customs and intelligence experts on the draft legal framework. The interviewees' opinion on some of these factors are discussed in Chapter Seven. The factors influencing new cooperation arrangements are not analysed extensively here. That is because the legal framework is designed to enable the automation of existing intelligence-sharing relationships. It is not intended to be a catalyst for developing new intelligence cooperation arrangements.

The independence-based factors affecting intelligence cooperation are "military cooperation, domestic regime types, cultural and economic characteristics, and ties to the international community".[189] Other factors include the alignment of political interests

[185] Russ Porter "Intelligence-led Policing and Public Trust" in Jerry Ratcliffe, *Intelligence-led Policing* (Willan, Devon UK, 2008) 222, at 223.

[186] Musa Tuzuner "The State-Level Determinants of the United States' International Intelligence Cooperation" (PhD Dissertation, Kent State University, 2009), at 9.

[187] Ratcliffe, above n 184, at 227 and Neil Walker "The Pattern of Transnational Policing" in Tim Newburn (ed) *Handbook of Policing* (Willan Publishing, Abingdon, 2008) 119, at 122.

[188] CarrieLyn Donigan Guymon "International Legal Mechanisms for Combating Transnational Organized Crime: The Need for a Multilateral Convention" (2000) 18(1) Berk J Intl L 53, at 54–55. Note however, at 73, Guymon suggests that INTERPOL be given greater powers to share information without the permission of individual states, which would conflict with the controls that the proposed legal framework aims to implement to ensure information is appropriately protected.

[189] Tuzuner, above n 186, at 9 and Stephane Lefebvre "The Difficulties and Dilemmas of International Intelligence Cooperation" (2003) 16(4) International Journal of Intelligence and CounterIntelligence 527, at 529.

and disparities in power between the parties.[190] Similarity of position in respect of each of these factors defines areas of common interest. This in turn influences the likelihood, extent and nature of intelligence cooperation. One example of this is the Five-Eyes agreement, discussed in Part IV of Chapter Five.

In respect of internal EU cooperation, Mesko and Furman stated:[191]

> To respond to certain types of security threats, the EU develops and accepts the key strategic documents that provide consistent approaches and activities of the competent authorities of the member states, and EU institutions, bodies, and agencies.

Policing networks may "involve networks which are relatively autonomous of [the] states of origin".[192] Bowling noted that, in the context of police intelligence cooperation, international police organisations and other cooperative arrangements are intended to transcend national differences.[193] For example, increased concern about the threat-based factors including international terrorism, organised crime, and the proliferation of weapons of mass destruction has led to an increase in security and intelligence cooperation across Europe and elsewhere.[194] This has resulted in greater surveillance and information analysis to detect and deter crime "without impeding legitimate cross-border exchange".[195] The Financial Action Task Force is another example of an initiative that has succeeded, perhaps due in part to a development process that was driven by "neutral, technocratic analysis, rather than by politics".[196]

---

[190] Jennifer E Sims "Foreign Intelligence Liaison: Devils, Deals, and Details" (2006) 19 International Journal of Intelligence and CounterIntelligence 195, at 198.

[191] Gorazd Mesko and Robert Furman "Police and Prosecutorial Cooperation in Responding to Transnational Crime" in Philip L Reichel and Jay S Albanese (eds) *Handbook of Transnational Crime and Justice* (Sage Publications, Thousand Oaks CA, 2014) 323, at 328. See also James Sheptycki "The Drug War: Learning from the Paradigm of Transnational Policing" in James Sheptycki (ed) *Issues in Transnational Policing* (Routledge, London, 2000) 201, at 214.

[192] Walker, above n 187, at 119 and 223.

[193] Ben Bowling "Transnational Policing: The Globalization Thesis, a Typology and a Research Agenda" (2009) 3(2) Policing: A Journal of Policy and Practice 149, at 150 and Alice Hills "The possibility of transnational policing" 19(3) Policing and Society: An International Journal of Research and Policy 300, at 301.

[194] Seniz Bigli "Intelligence Cooperation in the European Union: An Impossible Dream?" (January 2016) 5(1) All Azimuth 57, at 57 and Sir Stephen Lander "International Intelligence Cooperation: An Inside Perspective" (2004) 17(3) Cambridge Review of International Affairs 481, at 483. See also Bowling, above n 193, at 154 and Walker, above n 187, at 131.

[195] Peter Andreas and Ethan Nadelmann *Policing the Globe: Criminalization and Crime Control in International Relations* (Oxford University Press, New York, 2006), at 190.

[196] At 234.

The background of threat-based and independence-based factors contributes to a level of mutual trust between customs agencies that will determine whether cooperation will thrive or falter. However, another dynamic is that the system can be used by customs administrations to share intelligence that has been obtained from other sources. This presents challenges relating to secrecy and trust. Intelligence cooperation can also be hindered by concerns about a prospective intelligence partner's treatment of human rights.[197]

Hufnagel notes that the establishment of minimum standards for information exchange was an important factor in the context of European policing cooperation.[198] Endorsement, marking, special handling instructions and compartmentalisation are all terms used to describe the assigning of specific rules for the handling, storage and use of information.[199] It is essential that a customs administration handles the information it receives according these rules, in order to maintain the trusted information-sharing relationship. For example, information with a marking of "UK/NEW ZEALAND EYES ONLY" cannot be shared beyond authorised personnel in the United Kingdom and New Zealand. To do so would require a suitable authority in the originating state, in this case the United Kingdom, to first remove or amend the special handling instruction. Confidence that these rules will be followed is a prerequisite for any intelligence-sharing relationship. A failure to observe these rules could damage the trust that exists between customs administrations. It could also have the flow-on effect of damaging the trust that exists between the customs administration providing the information and the party from which it first received that information.

Equity is another possible factor influencing intelligence-sharing relationships. The relationships can be categorised as asymmetric, in which one party contributes more intelligence than it receives, or symmetric, in which each party contributes equally.[200] Anderson notes that:[201]

---

[197] Francesca Galli, Valsamis Mitsilegas and Clive Walker "Terrorism investigations and prosecutions in comparative law" (2016) 20(5) The International Journal of Human Rights 593, at 594.

[198] Saskia Hufnagel "'The Fear of Insignificance': New Perspectives on Harmonising Police Cooperation in Europe and Australia" (2010) 6(2) Journal of Contemporary European Research 165, at 166.

[199] New Zealand Security Intelligence Service *New Zealand Government Security Classification System* (NZSIS, Wellington, 2017), at 3.5 – 3.7, UK Government *Government Security Classifications April 2014* (Her Majesty's Stationery Office, London, 2013), at 11-12 and Ross J Anderson *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed, Wiley, Indianapolis, IN, 2008), at 243.

[200] Sims, above n 190, at 197.

[201] David Anderson QC *A Question of Trust: Report of the Investigatory Powers Review* (Her Majesty's Stationery Office, London, 2015), at para 10.31.

> Some of these [intelligence] relationships are broadly based where there is an enduring mutual interest. Others come together for a particular purpose such as a joint intervention.

In Europe, the development of these cooperative relationships has gone as far as a Council Framework Decision on joint investigation teams.[202]

Sims asserted that intelligence relationships should have an expectation of equity, meaning that each party to the intelligence relationship should make an equal contribution to the intelligence-sharing relationship over time.[203] Sims' view does not take into account the mutual benefit achieved when an intelligence partner acts against a common threat.[204] The reduction of a common threat, for example by shutting-down a drug cartel, or achieving an outcome that matches a shared goal of "politically, economically, culturally and socially inclusive global social order" can justify a mostly one-sided intelligence-sharing relationship.[205]

The harmonisation of laws is another important factor in policing cooperation.[206] Different policing methods hamper cross-border policing methods.[207] Work has already been done and continues to be done to harmonise international customs procedures.[208]

---

[202] Clive Walker "Clamping Down on Terrorism in the United Kingdom" (2006) 4(5) JICJ 1, at 14; Council Framework Decision on Joint Investigation Teams [13 June 2002] OJ L162/1; Michael Plachta "Joint Investigation Teams - A New Form of International Cooperation" (2005) 13(2) European Journal of Crime, Criminal Law and Criminal Justice 284, at 288 and 292; See also European Union Judicial Cooperation Unit "Joint Investigation Teams (JITs)" (7 November 2017) Eurojust <www.eurojust.europa.eu>.

[203] Sims, above n 190, at 198.

[204] Chris Clough "Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation" (2004) 17(4) International Journal of Intelligence and CounterIntelligence 601, at 604.The UN promotes cooperation in counter-terrorist activity: see Clive Walker "Investigative Journalism and Counter Terrorism Laws" (2017) 31(1) Notre Dame Journal of Law, Ethics and Public Policy 129, at 134 and *Security Council Resolition on Foreign Terrorist Fighters* S/RES/2178 (2014).

[205] James Sheptycki "The Constabulary Ethic and the Transnational Condition" in Andrew Goldsmith and James Sheptycki *Crafting Transnational Policing: Police Capacity-Building and Global Policing Reform* (Hart Publishing, Oxford, 2007), at 32–34, and Hills, above n 193, at 303.

[206] Hufnagel, above n 198, at 174.

[207] Saskia Hufnagel "Cross-Border Police Co-operation: Traversing Domestic and International Frontiers" (2011) 35 Crim LJ 333, at 334.

[208] For example, International Convention on the Simplification and Harmonisation of Customs Procedures (The Kyoto Convention) (1974) (deposited at the WCO, no document number, retrieved from www.wcoomd.org) and the International Convention on the Simplification and Harmonisation of Customs Procedures (as amended) (The Revised Kyoto Convention) (opened for signing 6 June 1999, entered into force 3 February 2006) (deposited at the WCO, no document number, retrieved from www.wcoomd.org).

The over-arching theme of the factors influencing intelligence cooperation is trust. Commonality of threats, military cooperation, domestic regime types, culture, economy, international ties and political interests all promote trust between intelligence partners.[209] Nonetheless, trust can be absent even when one or the majority of these factors are aligned. In the policing context:[210]

> Tension and friction continue to characterize many international police relations. Individual policemen may establish good relations with one another but police forces often fail to do so.

Actions by any party to an intelligence-sharing relationship can damage the trust that is foundation of the relationship, such as the inappropriate disclosure of classified information.[211] Past events can create an environment of mistrust within which new initiatives for intelligence cooperation cannot flourish.[212] This can affect domestic and international relationships. For example, pervasive distrust between the FBI and local law enforcement agencies inhibits intelligence cooperation in the United States.[213]

## *VIII Chapter Summary*

This Chapter provided an overview discussion of the types of information that need to be included within a legal framework for sharing customs intelligence through a single window system. The customs law enforcement and security risk-management process, the kinds of information needed in that process and the information standards that are currently used, were described.

Customs administrations perform risk-assessments to meet their responsibilities for law enforcement and national security relating to the cross-border movement of people, goods and craft. The law enforcement and national security responsibilities result in a need for information secrecy. That secrecy can erode public confidence, especially in times of crisis. In the late 19th century Lord Acton said:[214]

---

[209] For example, in the policing context, one state might use its police as a repressive apparatus to maintain authoritarian control, while another implements democratic control of the police. See Loader, above n 166, at 75 and 198. Differences like this, and their resulting effect on human rights and cultural similarity, could have a negative effect on trust between intelligence partners.

[210] Malcolm Anderson *Policing the World : Interpol and the Politics of International Police Co-operation* (Clarendon Press, New York, 1989), at 148.

[211] Sabrina Siddiqui and Ben Jacobs "Donald Trump 'Shared Highly Classified Information with Russian Officials'" *The Guardian* (online edition, Washington, 16 May 2017).

[212] Ratcliffe, above n 184, at 228.

[213] Ibid.

[214] Josef L Altholz, Damian McElrath and James C Holland (eds) *The Correspondence of Lord Acton and Richard Simpson Volume II* (Cambridge University Press, London, 1978), at 114.

> Everything secret degenerates, even the administration of justice; nothing is safe that does not show how it can bear discussion and publicity.

It creates fear that natural obligations of humanity and justice are being ignored and the rights and freedoms of individual are being secretly violated. Secrecy prevents the democratic participation of a constituency that is not fully informed of the actions and intentions of the state. Secrecy can prevent individuals from defending themselves against the abuse of their rights.

Furthermore, national security can be interpreted to include all aspects of safety, such as economic well-being. The various interpretations of security might be disputed by some members of the public and affect their confidence in the purposes of the proposed legal framework. This Chapter has not deeply examined nor offered normative statements on the definition of security as the aim of the thesis is to provide a practical means to share intelligence. It does not set out to evaluate the security responsibilities and propose changes to the role of customs. The thesis addresses only processes for intelligence-sharing and the subsequent use of intelligence. It does not cover the entire intelligence lifecycle, from its initial collection through to its eventual destruction. The focus of the thesis limits the effect that the proposed legal framework can have on public confidence in the protection of individuals' rights.

The next Chapter discusses the human rights affected by the proposed legal framework and for which transparency should exist.

# Chapter Three – Areas where Transparency can and should Exist

With an appropriate legal framework, the single window could be used to automate intelligence exchanges. Chapter Two provided an overview of the types of information that need to be included in the intelligence exchanges. It identified the essential operational requirements that customs administrations have for sharing intelligence. It described why secrecy about the information used by customs administrations can erode public confidence.

This Chapter builds on Chapter Two by identifying the privacy and other human rights that need to be protected in order to improve public confidence in intelligence-sharing by customs administrations. This Chapter supports the thesis by describing the rights that are covered by the measures set out in Chapter Five and that are addressed in the legal framework proposed in Chapter Seven.

The UN instruments for human rights are accepted here as benchmarks for their treatment. The human rights that are most likely to be directly or indirectly affected by the legal framework are identified. Cases are used as examples to illustrate the problems associated with the abuse of human rights, especially in law enforcement, security and intelligence contexts, both before and after these rights were set down by the UN. There are no normative claims made about the value of these human rights or the manner in which they are expressed.

Privacy is identified in this Chapter as the human right most affected by customs intelligence-sharing. Other human rights are affected only indirectly. Issues encountered in other intelligence and policing cooperation arrangements and their relevance to the proposed legal framework are discussed to provide context.

Greater evidence of human rights practices can improve public confidence in a government.[215] It is contended that the proposed legal framework can include this transparency without compromising the secrecy of information or customs intelligence collection, risk-management and law enforcement techniques.

There are seven Parts in this Chapter.

Part I describes why transparency is needed both to protect human rights and to promote public confidence.

[215] Chris Griffith "Australians Flock to VPNs to Avoid Data Retention" *The Australian Business Review* (online edition, Sydney, 13 August 2014), at 241; Sarah Joseph and Adam McBeth (eds) *Research Handbook on International Human Rights Law* (Edward Elgar Publishing, Cheltenham, 2010), at 426.

Part II discusses the right of access to justice. Access to justice is impeded when an individual is unaware of the existence of personal information that is used in judicial proceedings.

Parts III and IV explain that the use of information gained through illegal search and seizure or torture must also be transparently prevented.

Part V introduces the right to privacy. Privacy is a right that is very much affected by the proposed legal framework as it involves the sharing of personal information.

Part VI relates the need for government secrecy in intelligence-related activities to its effect on privacy and public confidence.

Part VII summarises the Chapter.

## *I The Consequence of Human Rights*

Transparent controls for the treatment of privacy and other human rights should improve public confidence in intelligence-sharing by customs administrations. This Part discusses the need for the transparent protection of human rights by providing some contextual information. It is not a comprehensive analysis of the origins and purpose of human rights, nor does it predict the extent to which public confidence will be improved by making the treatment of these rights evident in the legal framework.

The electorate of a state becomes untrusting of its government when it is apparent that human rights are being set aside.[216] This was observed in the 18th century, when Barrell noted that the trading-off of human rights for sovereign interests increased in times of international hostility:[217]

> The influence of the spirit of despotism had greatly increased in the three or four years prior to the writing of [Vicesimus Knox's] book, as a direct result of the war with France and the loyalist hostility to the rise of popular movements for the reform of parliament.

At the same time, criminologist and philosopher Beccaria was conflicted on the value of trading-off an individual's human rights against a utilitarian greater good. On the one hand, he stated:[218]

---

[216] Office of the United Nation's High Commissioner for Human Rights *Human Rights and Law Enforcement: A Trainer's Guide on Human Rights for the Police, Issue 5, Part 2* (United Nations, Geneva, 2002), at 16.

[217] John Barrell *The Spirit of Despotism: Invasions of Privacy in the 1790s* (Oxford University Press, Oxford, 2006). In this text, Barrell is referring to Vicesimus Knox *The Spirit of Despotism* (2nd ed, William Hone, London, 1821).

[218] Richard Bellamy (ed) *Beccaria: On Crimes and Punishments and Other Writings* (Cambridge University Press, Cambridge UK, 1995), at 101.

> It is a false idea of utility that gives higher importance to particular inconveniences than to the general inconvenience …. It is a false idea of utility that sacrifices a thousand real advantages for a single chimerical or unimportant disadvantage that would deprive men of fire because it burns or water because it drowns, and can only remedy evil by destruction.

On the other hand, Beccaria also put forward an argument against such trade-offs, saying "a useful injustice cannot be tolerated by a lawgiver who wishes to shut out the ever-vigilant tyranny".[219] English historian and parliamentarian Gibbon expressed a similar view in the 18th century:[220]

> The urgent consideration of the public safety may undoubtedly authorise the violation of every positive law. How far that or any other consideration may operate to dissolve the natural obligations of humanity and justice, is a doctrine of which I still desire to remain ignorant.

Writers such as Schmitt and Colon-Rios have more recently argued that legitimate political rule must conform to the will of the people.[221] Schmitt argued also that this legitimacy allows a sovereign authority to step outside of the rule of law in an emergency.[222] In the early 21st century, human rights trade-offs (the utilitarian perspective) were reflected in the policies of the George W Bush administration which allowed captives from the Iraq and Afghanistan conflicts to be imprisoned and interrogated without trial.[223] The United States Congress authorised the use of the executive power of the President to capture and detain unlawful combatants.[224] It is unsurprising that trade-offs of individual rights and freedoms occurred following the 9/11 terrorist attacks.[225] Opponents argued strongly against such human rights trade-offs and

---

[219] At 58.

[220] Edward Gibbon (originally published 1776) *The History of the Decline and Fall of the Roman Empire: A New Edition, In One Volume* (T Cadell, London, 1837), at 412.

[221] Carl Schmitt, Jeffrey Seitzer (translator) *Constitutional Theory (1928)* (Duke University Press, Durham NC, 2008), at 255; Carl Schmitt, Ellen Kennedy (translator) *The Crisis of Parliamentary Democracy (1923)* (MIT Press, Cambridge MA, 1985), at 109 and Joel Colon-Rios *Weak Constitutionalism: Democratic Legitimacy and the Question of Constituent Power* (Rutledge, Abingdon, 2012), at 7.

[222] Carl Schmitt, George Schwab (translator) *Political Theology: Four Chapters on the Concept of Sovereignty* (University of Chicago Press, Chicago, 2005), at 6.

[223] Jordan J Paust "Judicial Power to Determine the Rights and Status of Persons Detained Without Trial" (2003) 44 Harv Intl LJ 503, at 503.

[224] 115 Stat 224 Authorisation for the Use of Military Force (United States).

[225] George Duncan "Exploring the Tension Between Privacy and the Social Benefits of Government Databases" in Peter Shane, John Podesta and Richard Leone (eds) *A little knowledge: privacy, security and public information after September 11* (Century Foundation Press, New York, 2004) 71, at 81.

these opposing views were later endorsed by the Obama administration. [226]

These trade-offs occurred against a background of generally increasing state responses to humanitarian issues and transparent protection of human rights since the early 20th century.[227] Following the First World War, the Western allies sought a "lasting principle of self-determination" for the Eastern European nations.[228] This established a principle that sovereign states have an overarching responsibility to protect their own citizens and intervene on behalf of the citizens of other states.[229]

This principle aligns with Kant's ethical outlook which contends one should act only in a manner which would be acceptable as a universal law.[230] This is the basis of the European Convention for Human Rights.[231] Kant's categorical imperative insists a moral code should have no exceptions. People should always be treated with respect and dignity and always as an end in themselves, meaning their inherent value does not depend on anything else. Cropanzano and Grandly support this assertion that people can be treated as both a means and an end, but should never be used only as a means to an end.[232] This principle has been adopted by the UN Security Council in resolutions to intervene in sovereign states on behalf of the citizens of those states.[233]

The transparent protection of human rights must exist as an underlying goal for the proposed legal framework, recognising the non-binding aspiration created by the

---

[226] Executive Order 13492 Review and Disposition of Individuals Detained at the Guantanamo Bay Naval Base and Close of Detention Facilities 74 FR 4897, 27 January 2009 (United States), and Executive Order 13493 Review of Detention Policy Options 74 FR 4901, 27 January 27 2009 (United States).

[227] Daniel Philpott "Protection of Nations and Minorities: The Road to Versailles" in Sohail H Hashimi (ed) *State Sovereignty: Change and Persistence in International Relations* (Pennsylvania State Press, Pennsylvannia, 2010) 34, at 38.

[228] Ibid.

[229] Gareth Evans and Mohamed Sahnoun "The Responsibility to Protect" (2002) 81(6) Foreign Affairs 99, at 102.

[230] Immanuel Kant, James W Ellington (translator) *Grounding for the Metaphysics of Morals* (3rd ed, Hackett Publishing, Indianapolis, 1993).

[231] European Convention for the Protection of Human Rights and Fundamental Freedoms (The European Convention for Human Rights, or ECHR) UNTS 213 I-2889 222 (1950), in the preamble.

[232] Russel Cropanzano and Alicia Grandley "If Politics is a Game, Then What are the Rules?: Three Suggestions for Ethical Management" in Marshall Schminke (ed) *Managerial Ethics: Moral Management of People and Processes* (Lawrence Erlbaum & Associates, Mahwah NJ, 1998) 133, at 150.

[233] Some examples are and *Security Council Resolution on Measures to Guarantee the Safety and Protection of the Palestinian Civilians in Territories Occupied by Israel* S/RES/904 (1994); *Security Council Resolution on the Responsibility to Protect Civilians* S/RES/1265 (1999); *Security Council Resolution Reaffirming the Responsibility to Protect Civilians* S/RES/1296 (2000); *Security Council Resolution Reaffirming the Responsibility to Protect Civilians* S/RES/1674 (2006) and *The Situation in Libya* S/RES/1973 (2011).

Universal Declaration of Human Rights (UDHR) which states:[234]

> … every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance….

This principle is enshrined in the International Covenant on Civil and Political Rights (ICCPR), which states:[235]

> Recognizing that, in accordance with the Universal Declaration of Human Rights, the ideal of free human beings enjoying civil and political freedom and freedom from fear and want can only be achieved if conditions are created whereby everyone may enjoy his civil and political rights, as well as his economic, social and cultural rights.

These rights continue to be elaborated and enacted in domestic and international legislation, and development in non-governmental documents such as the Johannesburg Principles.[236] The Johannesburg Principles were developed by a human rights activism and charity group, Article 19, as a statement of principles that it believes should apply in a national security context. The Johannesburg Principles were developed with the awareness that "some of the most serious violations of human rights and fundamental freedoms are justified by governments as necessary to protect national security".[237]

To ensure the on-going trust and confidence between states, and to maintain public confidence in the state, no provision of the intelligence-sharing system should violate the commonly accepted human rights. Transparent mechanisms must exist that enable these rights to be recognised and promoted.

## *II The Right of Access to Justice*

This Part discusses the need for the protection of the right to access to justice to be visible to the public. Articles 9, 14, 16 and 26 of the ICCPR describe the rights of individuals to

---

[234] *Universal Declaration of Human Rights* GA Res 217A, A/RES/3/217 A (III) (1948) (UDHR), from the preamble.

[235] International Covenant on Civil and Political Rights GA Res 2200A, A/RES/21/2200 (1966) (ICCPR), from the preamble.

[236] For example, New Zealand Bill of Rights Act 1990, ECHR, above n 231, and "The Johannesburg Principles on National Security, Freedom of Expression and Access to Information" (1996) Article 19 <www.article19.org>.

[237] Article 19, above n 236, at 6 and principle 1(d).

a fair hearing.[238] It is essential this right is protected in the legal framework, as the violation of these rights is incompatible with the UDHR, the Charter of the UN, and the rules of natural justice.[239] The discussion in this Part provides some background and examples of why the inclusion of this right in the legal framework is important. It does not describe the evolution or all the aspects of this right, evaluate its worth, nor establish the potential effect on public confidence of its inclusion in the legal framework.

The vilification of totalitarian governments that use surveillance, secret denunciations and denial of access to justice was described in the 18th century by Beccaria as a form of tyranny:[240]

> Who can defend himself against false accusation when it is guarded by tyranny's strongest shield, secrecy? What sort of government can it be in which the ruler suspects every subject of being an enemy, and is forced to preserve the public peace by taking away each individual's peace of mind?

In the last hundred years, this has been reflected numerous times in literature, such as *The Trial*, a novel first published in 1925 in which the protagonist tries to find out why the court is interested in his life, but finds the court is too clandestine and complex to be fully understood. Kafka described a bureaucracy that worked in a secretive and mysterious way, completely unaccountable and amoral.[241] Similarly, in Orwell's futuristic novel *Nineteen Eighty-Four*, the fictional society ruled over by the authoritarian and oppressive dictator called "Big Brother" is commonly cited as an example of a dystopia.[242]

Despite this, it must be recognised that intelligence-sharing is typically conducted in secret so that governments can protect:

(a) The identity and safety of the individuals that provide the intelligence to government;[243]

(b) The effectiveness of criminal investigations, which would be compromised if criminals became aware of the information that investigators held about them

[238] ICCPR, above n 235, arts 9, 14, 16 and 26, implemented in the New Zealand Bill of Rights Act 1990 (New Zealand), ss 23–27.

[239] See the preamble of the Charter of the United Nations and Statute of the International Court of Justice UNTS 1 (opened for signing 26 June 1945, entry into force 24 October 1945).

[240] Bellamy, above n 218, at 37.

[241] Breon Mitchell (translator) *The Trial/Franz Kafka: A New Translation Based on the Restored Text* (Schocken, New York, 1998).

[242] George Orwell *Nineteen Eighty-Four* (Secker & Warburg, London, 1949).

[243] For example, see Privacy Act 1993 (New Zealand), s 27 (d) and 5 USC § 552 s (b) (7) (D).

and their activities;[244] and

(c) The effectiveness of intelligence, investigation and law enforcement methods, which criminals would try to circumvent if they gained detailed knowledge of how these work and the information they gain.[245]

In this environment of secrecy, provisions for access to justice are needed to fulfil the requirements of the ICCPR. Article 14, which provides an entitlement to a public hearing, may not always be appropriate where a need for secrecy exists.[246] The New Zealand Privacy Commissioner recognised this in 1999, stating:[247]

> As Privacy Commissioner, I have repeatedly recommended enhancements to accountability mechanisms …. As much of the work of the NZSIS must be carried out in secret, it is sometimes difficult for normal accountability mechanisms to work in a completely open fashion. However, parliamentary reporting is possible while taking into account the need for security.

Secrecy for security purposes in immigration decision-making is a relatively recent development. Before 1999, individuals being deported were entitled to know all the evidence against them.[248]

In 1999, Part 4A was added to the Immigration Act 1987.[249] Part 4A enabled the Director of Security to issue a security risk certificate on the basis of classified information, without divulging that classified information.[250] A security risk certificate could certify that an individual's continued presence in New Zealand constituted a threat to national security.

---

[244] For example, see Privacy Act 1993 (New Zealand), s 27 (c) and 5 USC § 552 s (b) (7) (A).

[245] For example, see United States National Security Council, above n 150. See also 5 USC § 552 s (b)(7)(E) and *Hunt v Central Intelligence Agency* 981 F 2d 1116 (1992).

[246] The right to access to justice can be considered alongside the protection from arbitrary arrest and detention. Arbitrary arrest and detention and the denial of access to justice are denials of an individual's freedom and security of person. While art 9 of the UDHR which simply states "No one shall be subjected to arbitrary arrest, detention or exile", art 9 of the ICCPR includes the right of an individual to be informed of the reason for the arrest, the right to prompt judicial proceedings and the right to compensation for unlawful arrest or detention.

[247] Bruce Slane "SIS to Report Publicly for the First Time NZSIS (No 2) Bill" (20 July 1999) Privacy Commissioner <privacy.org.nz>.

[248] Lani Inverarity "Immigration Bill 2007: Special Advocates and the Right to be Heard" (2009) 40 VUWLR 471, at 472. See also Immigration Act 1987 (New Zealand).

[249] Immigration Amendment Act 1999 (New Zealand).

[250] The Director of Security is head of the New Zealand Security Intelligence Service (the NZSIS).

This law was tested in the case of Ahmed Zaoui, an Algerian national. Zaoui applied for refugee status on arrival in New Zealand in December 2002.[251] The Director of Security issued a security risk certificate in respect of Zaoui. That certificate was reviewed by the Inspector-General of Security.[252] Zaoui's initial application for refugee status was approved in August 2003, but he remained in detention until December 2004 while the Minister of Immigration considered the security risk certificate.[253] Judicial review of Zaoui's case continued until the security risk certificate was withdrawn by the Director of Security in September 2007.[254]

A central issue in the judicial review was the need to balance the secret issues identified in the security risk certificate against the need to protect human rights, in that case in the context of art 33 of the Refugee Convention.[255] It has been argued that, even in an environment of absolute secrecy, every individual should have fair and equitable access to justice in cases where secret intelligence is allegedly used to breach that individual's human rights.[256]

It is contended here that transparency should exist in the state's use of intelligence for customs purposes. Individuals should have the ability to know of and challenge intelligence in judicial proceedings. As a result, the proposed legal framework has transparent conditions that allow any information that is shared to be used as evidence in judicial proceedings and challenged by the defendant. Nevertheless, the cases of *Zaoui* and *Tele2 Sverige and Secretary of State for the Home Department v Post- och telestyrelsen and Others* illustrate that in some security and law enforcement cases, information should be withheld from the information subject.[257] In New Zealand, the ability to keep information secret from the data subject in some circumstances is allowed through legislation such as s 25 of the Privacy Act 1996, s 7 of the Immigration Act 2009,

[251] *Zaoui,* above n 159.

[252] Inspector-General of Intelligence and Security Act 1996 (New Zealand), s 4. The Inspector-General of Security is a statutory role established to ensure the activities of the NZSIS comply with the law

[253] Television New Zealand "Timeline in the Ahmed Zaoui Case" (9 July 2007) Television New Zealand <tvnz.co.nz>.

[254] David Cunliffe "Ahmed Zaoui Statement" (14 September 2007) New Zealand Government <beehive.govt.nz>.

[255] *Zaoui v Attorney-General* [2005] 1 NZLR 690, at 28 and Convention and Protocol Relating to the Status of Refugees 189 UNTS 137 (entered into force 22 April 1954) (Refugee Convention).

[256] Ibid and Emma Bell *Soft Power and Freedom Under the Coalition: State-Corporate Power and the Threat to Democracy* (Palgrave MacMillan, Basingstoke, 2015), at 60.

[257] *Zaoui v Attorney-General*, above n 255, and Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Secretary of State for the Home Department v Post- och telestyrelsen and Others* [2016] ECR 970.

s, s 38M(7) of the Customs and Excise Act 1996 and s 6 of the OIA. The legal framework proposed here does not provide a mechanism to defeat those provisions.[258]

### *III Protection from Arbitrary Search and Seizure*

This Part discusses the need for openness in the legal framework in respect of the right to protection from arbitrary search and seizure and the means through which this openness will be achieved in the proposed legal framework. Protection from arbitrary or unreasonable search and seizure is an issue of constitutional importance. It is not an explicit right established in the ICCPR, although art 17 provides everyone with protection from "arbitrary or unlawful interference with his privacy, family, home or correspondence".[259] The right of protection from arbitrary search and seizure is related to the right of privacy because an individual may have an expectation of privacy for the information and items discovered during a search and seizure. This right exists in the domestic law of New Zealand and some other states.[260] Some examples from UK and New Zealand law are provided here for context, but the discussion is neither a complete analysis of these examples, nor is it a comprehensive analysis of the right.

Protection against unlawful search and seizure in the context of free speech and state necessity was established in English Common Law in *Entick v Carrington*.[261] In 1762, Great Britain was in political turmoil, with hostility between Hanoverians and Jacobites, between Whigs, who supported the King, and Tories and between Roman Catholics and Anglicans.[262] Entick was a writer of the broadly anti-government weekly paper called

---

[258] Changes to the treatment of national security information have been recommended in New Zealand Law Commission "The Crown in Court: A review of the Crown Proceedings Act and National Security Information in Proceedings (R135)" (2015) New Zealand Law Commission <www.lawcom.govt.nz>. Recommendations include, at para [5.50], procedures in the discovery phase of civil proceedings that would enable the non-Crown party to challenge the non-disclosure of security information. The court would consider, in closed session, whether the information can be fairly excluded from proceedings. The New Zealand Law Commission also recommends, at para [5.59], the use of special advocates to represent the defendant's interests in pre-trial stages of criminal cases and help the judge to determine whether information should be withheld. The special advocate would be present in court when the defendant is excluded from the stages of the process that involve national security information.

[259] ICCPR, above n 235.

[260] For example, the New Zealand Bill of Rights Act 1990, s 21; Constitution (Costituzione Della Repubblica Italiana) 1947 (Italy), art 13; and the Fourth Amendment to the United States Constitution (1792) (United States).

[261] *Entick v Carrington* (1765) 19 St Tr 1030, (1765) 19 St Tr 1029, [1765] EWHC KB J98, [1558-1774] All ER Rep 41, 95 ER 807.

[262] David Feldman "The Politics and People of Entick v Carrington" in Adam Tomkins and Paul Scott (eds) *Entick v Carrington: 250 Years of the Rule of Law* (Hart Publishing, Oxford, 2015) 5, at 5–12.

*The Monitor*.[263] Beardmore was implicated in the publication of the same paper and he and Entick were both supporters of Wilkes, an MP and publisher of another anti-government paper called *The North Briton*.[264] The case of *Entick v Carrington* was contemporaneous with cases involving Wilkes, Beardmore and others, including printers that were arrested after being incorrectly identified as involved in publication of seditious material.[265] Entick was accused by the Secretary of State of writing seditious papers. He was subjected to a search of his home, seizure of property and property damage by Carrington, the King's chief messenger, and other messengers. The messengers were acting on the orders of, and under a general warrant issued by, the Secretary of State for the Northern Department. The general warrant named Entick, but was non-specific in regard to the goods that were to be seized. The warrant included an instruction to seize all of Entick's books and papers, rather than any particular books or papers that were evidence of sedition.

Lord Camden CJ found in favour of Entick, declaring that there was nothing in statute or Common Law which gave the Secretary of State the power to issue such a warrant, saying:[266]

> If libels may be seized it ought to be laid down with precision, when, where, upon what charge, against whom, by what magistrate, and in what stage of the prosecution. All these particulars must be explained and proved to be law, before this general proposition can be established.

Accordingly, Lord Camden CJ found that the general warrant issued by the Secretary of State was illegal and void.

Similarities can be drawn between *Entick v Carrington* and *Dotcom v Attorney-General*.[267] The *Dotcom* case is relevant to this study as it involves both the gathering and sharing of intelligence. In the *Dotcom* case, the role of the King's chief messenger and messengers was played by the New Zealand Police and GCSB. In *Dotcom*, the Police also shared the role of Halifax with the United States FBI. The FBI accused Dotcom of copyright infringements and sought his extradition to the United States. The New Zealand Police obtained and executed a search warrant on Dotcom's property with the assistance of the GCSB. The GCSB gathered intelligence on Dotcom through electronic surveillance, which it shared with the Police. Dotcom's assets were seized by the police.

---

[263] At 26.

[264] Ibid.

[265] At 30–35 and 37–40.

[266] *Entick v Carrington* (1765) 19 St Tr 1030, (1765) 19 St Tr 1029, [1765] EWHC KB J98, [1558-1774] All ER Rep 41, 95 ER 807.

[267] *Dotcom v Attorney-General* [2012] NZHC 1494, [2012] 3 NZLR 115.

Winkelmann J found the search warrant to be unlawful, a view which was overturned on appeal.[268] Furthermore, GCSB's surveillance of Dotcom was found to be unlawful because it relied on incorrect information regarding Dotcom's immigration status.[269]

Another example is the European Court of Human Rights case of *Malone v United Kingdom,* which found the United Kingdom had breached Malone's right to privacy in intercepting his postal and telephone communications for intelligence purposes.[270] The Court also found that there had been a breach of Malone's rights in UK domestic law did not provide an "effective remedy before a national authority" in respect of the interceptions carried out under warrant.

The fundamental civil and political human rights and freedoms of individuals are enshrined in the ICCPR. Even so, the right to protection from arbitrary or unlawful search and seizure is not explicitly set out in the ICCPR, although it is self-evident in the wording of the privacy article:[271]

> … no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence ….

An arbitrary search and seizure of, say, the contents of an individual's pockets or home would be an unlawful interference with the privacy right expressed in the ICCPR article.

This right should be protected in the domestic legislation and the constitutional framework that establish the rule of law in participating states. This right can be considered as an extension of the right to privacy. Recognising this, the proposed legal framework does not impose any particular protection from arbitrary or unlawful search and seizure. Instead, it enables states to act with autonomy, but under the terms of the existing international human rights Conventions and the scrutiny of the organisations established for this purpose. It does this by requiring states to supply or accept only information that has been lawfully obtained.

---

[268] Ibid. The decision on the search warrant was subsequently overturned in *Attorney-General v Kim Dotcom* [2014] NZCA 19 in which Ellen France, Randerson and White JJ ruled that the general description of the items to be seized "was as specific as could reasonably be expected in the circumstance", at [47] and [53]. The Justices also ruled, at [48], that, contrary to Winkleman J's views in *Dotcom v Attorney-General* [2012] NZHC 1494, [2012] 3 NZLR 115 at [84] and [86], conditions did not need to be imposed on the forensic copying (cloning) of data. The Justices did, however, uphold Winkleman J's declaration that the removal of the cloned copies of Dotcom's computer data to the United States was unlawful, at [114].

[269] *Dotcom v Attorney-General* [2013] NZHC 1269; *Dotcom v Attorney-General* [2014] NZSC 199; "GCSB acted illegally on Kim Dotcom" (2013) Fairfax Media <www.stuff.co.nz> and Rebecca Quilliam "Kim Dotcom Loses Search Warrant Fight" *The New Zealand Herald* (online edition, Auckland, 23 December 2014).

[270] *Malone v United Kingdom* [1985] ECHR 5, (1984) 7 EHRR 14, [1984] ECHR 10.

[271] ICCPR, above n 235, art 17.

## *IV Freedom from Torture*

This Part discusses the need for the proposed legal framework to include transparent protection of the right to freedom from torture. This right is relevant because torture is sometimes used to obtain intelligence.[272] The use of unlawful methods such as torture to obtain intelligence is at odds with the purpose of the proposed legal framework, which is to improve public confidence through better treatment of human rights.[273] However, the right is not directly affected by the legal framework, which aims to automate the sharing of customs intelligence that has already been collected. Torture is an abuse of rights that can occur during the collection of information. The collection phase of the intelligence lifecycle is not addressed by the legal framework.

There has long been widespread public condemnation of torture, but it remains prevalent in modern society.[274] Society's aspirations for the abolition of torture, against which international agreements should be measured, are evident in historical literature and contemporary domestic and international law.

The literature of the 18th century records the abhorrence or abolition of torture in many Western states. In the 18th century, Beccaria condemned the use of torture to extract a

---

[272] Philip N Rumney *Torturing Terrorists: Exploring the Limits of Law, Human Rights and Academic Freedom* (Routledge, Abingdon, Oxon, 2014), at 84.

[273] The legal framework cannot guarantee the compliance of customs administrations to its terms. The legal framework is not aimed at changing the fundamental basis upon which existing intelligence-sharing agreements have been made. It relies upon self-reporting customs administrations and the effectiveness of an internal data controller. Reliance on the oversight of an independent third party is insufficient because the nature of intelligence work precludes independent third parties from having access to all the intelligence that a customs administration may possess. For example, the New Zealand Inspector-General of Intelligence and Security, is an independent oversight body for the NZSIS. The Inspector-General stated that the NZSIS impeded the its inquiry into NZSIS's unlawful access to New Zealand Customs Service data. This was reported in Inspector-General of Intelligence and Security "Annual Report for the Year Ended 30 June 2017" (2017) Office of the Inspector-General of Intelligence and Security <www.igis.govt.nz>, at 16. The importance of oversight is discussed in Chapter Four.

[274] For example, United Kingdom Joint Committee on Human Rights *Allegations of UK Complicity in Torture: Twenty–third Report of Session 2008–09* (Her Majesty's Stationery Office, London, 2009) which recommended an independent inquiry to investigate allegations of torture; Sir Peter Gibson *The Report of the Detainee Inquiry* (Her Majesty's Stationery Office, London, 2013), at [7.6], which found that UK personnel were at least "aware of inappropriate interrogation techniques and mistreatment of prisoners" and the award of damages for the United Kingdom's complicity in the torture done by authorities of the United States in *Binyam Mohamed v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 65, [2009] EWHC 152 (Admin), [2008] EWHC 2048, 2100, 2519, 2549, 2973 (Admin). Torture is uncommon in the New Zealand Customs Service and the government of New Zealand, as evidenced by the *Human Rights Council: Report of the Working Group on the Universal Periodic Review - New Zealand* A/HRC/26/3/Add 1 (2014), the most recent UN periodic review of human rights, which states "In response to a comment from Iran (Islamic Republic of), New Zealand reaffirmed that torture did not occur in New Zealand", at 10.

confession:[275]

> No man can be called guilty before the judge has reached his verdict; nor may society withdraw its protection from him until it has been determined that he has broken the terms of the compact by which that protection was extended to him. By what right, then, except that of force, does the judge have the authority to inflict punishment on a citizen while there is doubt about whether he is guilty or innocent?

Bonaparte remonstrated against the use of torture in that same century.[276] Frederick II of Prussia abolished most forms of torture in 1740.[277] However, there was at the same time a commonly held acceptance of torture in both military and civil contexts. Beccaria recognised the application of torture to gain intelligence. He noted torture was an accepted practice to extract information from an accused about accomplices.[278] That is, even after a criminal has confessed or despite the absence of a confession, he or she may still render information that points to the guilt of another. Although Frederick II of Prussia abolished torture to extract confessions, that was only in non-military cases.[279] A century later, France abolished the state use of torture.[280]

Torture in military contexts has been tolerated or condoned many times in recent history. For example, in the 1950s, the French police and army were authorised to extract information "by any means necessary, including torture" from FLN guerrillas.[281] In such circumstances the purpose of torture is not to extract confessions, but is instead used to identify and eliminate the enemy.[282]

Democracy and torture coexist and, in some cases, systematic torture has continued to occur in democracies where "…an objective or perceived national threat was absent".[283] Nonetheless, both the past approaches and any proposed international Convention for

[275] Bellamy, above n 218, at 39.

[276] John Eldred Howard (ed) *Napoleon Bonaparte: Letters and Documents of Napoleon, Volume I: the Rise to Power* (The Cresset Press, London, 1961).

[277] Bellamy, above n 218, at xxxv.

[278] At 39.

[279] At xxxv.

[280] Déclaration des droits de l'homme et du citoyen 1789, art IX.

[281] Darius Rejali *Torture and Democracy* (Princeton University Press, New Jersey, 2007), at 46.

[282] Tzvetan Todorov "Torture in the Algerian War" (2002) Summer (135/136) Sagalmuni 15, at 17.

[283] Rejali, above n 281, at 22.

sharing intelligence must be evaluated against society's aspirations for the abolition of torture. In this regard, Rejali observed: [284]

> …most states perceive the advantages of at least appearing to respect human rights". Even repressive states know that bad publicity and human rights monitors can undermine their legitimacy, commerce and the foreign aid on which they depend.

In contrast, modern history has recorded many attempts to put an end to the torture of prisoners. For example, art 7 of the ICCPR states:[285]

> No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected without his free consent to medical or scientific experimentation.

The prohibition is covered in more detail by the UN Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Convention Against Torture).[286] These Conventions elaborate on terms of the earlier Convention Relative to the Treatment of Prisoners of War (the third Geneva Convention) that were specific to the treatment of prisoners of war.[287] The ICCPR and the Convention Against Torture extend protections against torture to all individuals in all circumstances.

Some qualified public support for torture still exists despite the development of international law prohibiting all forms of torture, arbitrary arrest and detention. This is perhaps due to the need discussed above to gain intelligence from accused and confessed offenders. Polls indicate that almost half of the people in the United States believe torture is justified to gain important information from terrorists. [288] Also, while a body of international law exists to prohibit the execution of torture, prohibitions against less direct involvement are unclear.

In this regard, the Convention Against Torture states:[289]

> For the purposes of this Convention, torture means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person… when such pain or suffering is inflicted by or at the instigation of or

[284] At 26.

[285] ICCPR, above n 235, art 7.

[286] Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment UNGA Res 39/46, A/Res/39/46 (1975) (Convention Against Torture).

[287] Convention Relative to the Treatment of Prisoners of War 75 UNTS 135 (1950).

[288] Editorial "Spies, Torture and Terrorism: The Dark Pursuit of Truth" *The Economist* (online edition, London, 30 July 2009) at 20, at 20.

[289] Article 1 (1).

> with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions.

In the context of intelligence-sharing, consent or acquiescence might include a state official receiving and using intelligence that he or she suspects may have been gained through the application of torture.[290] For example, it is foreseeable that a state would accept intelligence it suspects may have been gained through the arbitrary arrest, detention and torture of an individual by another state, if that intelligence would help prevent an imminent terrorist act involving significant loss of life. In this example, accepting the intelligence would be the lesser of two evils as many lives would be saved at the cost of the freedom and welfare of a single individual. This is a utilitarian approach. A definition of consent or acquiescence that limits complicity to only knowing, and not just suspecting, that torture has occurred might be too broad, as the focus of the Convention Against Torture is to require a state party to "take effective legislative, administrative, judicial or other measures to prevent acts of torture in any territory under its jurisdiction".[291]

The analysis above reveals two distinct conditions for prohibitions against torture, arbitrary arrest and detention when analysing intelligence-sharing arrangements. Provisions should provide states with the ability to demonstrate compliance with both international law and prevailing public opinion. At first sight, such provisions may appear pointless because it seems unlikely that any offending state would freely admit the intelligence it shares has been gained through arbitrary arrest, detention and torture.[292] The distribution of information about the state's human rights abuses is essential to the progressive reform of abusive states.[293] A denial can be indicative of the early phases that

[290] In the United Kingdom, there is explicit policy for intelligence officers and service personnel which prohibits this in "Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees" (2010) United Kingdom Cabinet Office <www.gov.uk>, at [6], [7] and [9], and more general risk-management guidance for other government personnel in "Overseas Security and Justice Assistance Guidance (OSJA): Human Rights" (2017) Foreign & Commonwealth Office <www.gov.uk>, at 12.

[291] Article 2 (1).

[292] For example, see Gordon Corera "No Collusion in Torture, says MI6 Chief" (10 August 2009) BBC News <news.bbc.co.uk>. See also Robert Verkaik "Minister's Admission Links MI5 and MI6 to 'Torture Victim'" *The Independent* (online edition, London, 10 April 2009).

[293] Diana Halloy "Human Rights During Argentina's Military Rule: The Politics of Forced Disappearances" (the 2nd Global International Studies Conference, Ljubljana, 2008), at 2 and Cosette Creamer and Beth A Simmons "Does Self-Reporting Matter? Evidence from the Convention Against Torture" (20 April 2015) Harvard University <scholar.hardvard.edu>

a state goes through as it progresses towards respecting human rights.[294] Accordingly, rules should and do already exist for states to self-report torture and other human rights abuses, or for other states to raise concerns about abuses.[295]

Protection against torture must also exist in the domestic law of those states that are signatories to the Convention Against Torture. For example, in New Zealand the Evidence Act 2006 states evidence is unlawfully obtained and therefore inadmissible if:[296]

> … it is obtained in consequence of a breach of any enactment or rule of law by a person to whom s 3 of the New Zealand Bill of Rights Act 1990 applies.

Furthermore, s 9 of the New Zealand Bill of Rights Act 1990 states:

> 9. Right not to be subjected to torture or cruel treatment
>
> Everyone has the right not to be subjected to torture or to cruel, degrading, or disproportionately severe treatment or punishment.

In regard to applicability of this legislation:[297]

> This Bill of Rights applies only to acts done—
>
> (a) by the legislative, executive, or judicial branches of the Government of New Zealand; or
>
> (b) by any person or body in the performance of any public function, power, or duty conferred or imposed on that person or body by or pursuant to law.

The use of evidence gained through torture would therefore be inconsistent with New Zealand domestic law and international prohibitions against complicity in torture.[298] In this regard, the Convention Against Torture explicitly states that:[299]

> Each state party shall ensure that any statement which is established to have been made as a result of torture shall not be invoked as evidence in any

[294] Ibid.

[295] Optional Protocol to the Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment A/RES/57/199 (opened for signing 18 December 2002, entered into force 22 June 2006), arts 1 and 19.

[296] Evidence Act 2006 (New Zealand), s 30(5).

[297] Section 3.

[298] Convention Against Torture, above n 286, art 4.

[299] Article 15.

> proceedings, except against a person accused of torture as evidence that the statement was made.

Accordingly, the proposed legal framework has a condition that implicitly condemns torture through a requirement that only lawfully collected intelligence may be shared.

## *V Privacy, Law Enforcement and Security*

This Part discusses the privacy exemptions that cover personal information in some law enforcement and national security activities and the effect of that those exemptions on privacy and public confidence. The importance of including transparent privacy protections to improve public confidence in the legal framework is established.

Law enforcement and national security activities are exempted from privacy law in many states. To give three examples:

One, the privacy provisions of the EU Data Protection Directive do not apply to the processing of personal data for state security matters and state activity in areas of criminal law.[300]

Two, the New Zealand privacy law and customs law provide exemptions for information relating to security and law enforcement.[301] The OIA also includes security and maintenance of the law as reasons for withholding information.[302]

Three, individuals are not afforded any rights to privacy by the United States PATRIOT Act, which establishes broad powers for intelligence collection and sharing by government agencies in order to combat terrorism.[303]

These exemptions allow the state some autonomy when using personal information in activities to protect the security of the state.

Despite these exemptions, intelligence is not always easily shared between or even within states. The government agencies that use intelligence are protective of the data they hold and the means they use to collect them. This was witnessed by Theoharis, who wrote that the 1964 – 1972 Cold War era conflict between the FBI and the Central Intelligence Agency (CIA) was the result of "irrational suspicions, bordering on paranoia, of CIA

[300] Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31, art 3 (2).

[301] For example, Privacy Act 1993 (New Zealand), s 6 Principle 2(2) and s 27 and Customs and Excise Act 1996 (New Zealand), s 282A(2).

[302] OIA, s 6.

[303] 115 Stat 272 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001 (The PATRIOT Act) (United States).

counterintelligence chief [James] Angleton".[304] This is amplified at the border, as noted by Bashford:[305]

> Drawing borders around territory to produce 'us' and 'them' does not simply reflect divisions, but also helps to create heirarchised [sic] differences. As Augé remarks, it is intolerance and fear of the other that itself creates and structures nationalism and regionalism.

This reflects the territorial aspect of sovereignty and the regional context in which a struggle exists for "justice, participation, political power and resources".[306] This Chapter previously discussed how states might secretly collect and use personal information to pursue their political power and economic interests. Such manipulation could conflict with the desires for justice and participation.[307] For example, the manipulation of intelligence-sharing would conflict with the desire for justice, if that manipulation violates human rights. Likewise, the desire for participation in intelligence-sharing arrangements could be reduced because of the risk of manipulation.

Part IV of Chapter Two discussed how the trading-off of personal interests for the state interests could be enabled by the broad powers granted to customs administrations through legislation. Although such trade-offs undoubtedly occur from time to time, they must be limited to ensure the on-going stability of governments. In this regard, the people in a democracy such as the United States vest in their government only those powers "as may, from time to time, be deemed wise and necessary".[308] Thus, if the people deem a government's use of powers sufficiently unwise or unnecessary, a new government will be elected to revoke the powers or change the way they are used. Colon-Rios describes this as the difference between the constituent power held by the people and delegate power conferred by the people on their government.[309]

The state must balance an individual's right to privacy with the state's obligations to other citizens, states and businesses. In the event that a customs administration fails to meet these obligations, undesirable consequences may follow. For example, if a customs

---

[304] Theoharis, above n 132, at 167.

[305] Alison Bashford *Medicine at the Border: Disease, Globalisation and Security, 1850 to the Present* (Palgrave Macmillan, Basingstoke, 2006) and Marc Augé *A Sense of the Other* (Stanford University Press, Palo Alto, 1998), at 106.

[306] Francis Mading Deng, Sadikiel Kimaro, Terrence Lyons and others *Sovereignty as Responsibility: Conflict Management in Africa* (The Brookings Institution, Washington DC, 1996), at 132.

[307] Ibid.

[308] Sutherland, above n 163, at 25.

[309] Joel Colon-Rios "Five Conceptions of Constituent Power" (2014) 130 LQR 306, at 306, citing Dr Young's Letter (1777).

administration fails to meet its obligations to adequately protect intelligence, the agencies of foreign states could choose to cease providing intelligence. Similarly, customs administrations must be careful when meeting their obligations to their parent governments to report on the effectiveness of intelligence in risk-targeting and interventions. For example, the New Zealand Customs Service reports annually to parliament on the provision of intelligence and risk-assessments that inform intervention strategies, including alerts for goods, people and craft.[310] Customs administrations must also take care not to disclose sensitive intelligence methods or sources, or private or commercially sensitive information when making these reports.

Each customs administration is obliged to protect the safety and general well-being of its intelligence sources. The state must protect the anonymity of individuals who disclose information about drug crime, because threats, physical harm and loss of life may follow if the identity of those individuals becomes known. Similarly, a trader may suffer economic harm through a loss of customers if it becomes known that the trader was a source of customs intelligence. This would disadvantage that trader and provide advantage to its competitors, creating a disincentive for other traders to cooperate with customs and other government agencies in law enforcement initiatives.

Customs administrations must also protect individuals and traders who are the subjects of intelligence. Individuals may suffer threats to their safety and well-being to the subject of the information if their personal information or the fact that they are the subject of an intelligence holding or customs investigation is inappropriately disclosed. Similarly, traders may suffer economic loss if their commercially sensitive information is disclosed. Losses can additionally arise from disclosure that a trader is the subject of customs intelligence or the subject of an investigation.

Damage can also occur to businesses and individuals as the result of poor quality intelligence data. In this regard, Schermer argues that, “due to the nature of single window facilities it is possible that reuse of incomplete, inaccurate, or incorrect data could lead to multiple instances where damages are incurred”.[311]

If a customs administration breaches its duty to a private individual or business, it may incur tortious liability for damage suffered. Public officials who have acted outside their legal authority or who disregard the privacy of individuals may find themselves criminally liable and the customs administration may be civilly liable for any damage caused. For example, recording, copying or disclosing information that is likely to prejudice the security or defence of New Zealand and the corrupt use of official

[310] For example, New Zealand Customs Service *Annual Report 2015/16* (New Zealand Customs Service, Wellington, 2016).

[311] Bart W Schermer "Legal Issues of Single Window Facilities for International Trade" (2007) UNCITRAL <uncitral.org>.

information are criminal offences.[312] Also, a customs officer would be criminally liable for knowingly disclosing information obtained from customs' computer systems for an unauthorised purpose.[313] If he or she in so doing also did know or should have known that this could result in damage to the subject of the intelligence, then that could give rise to the tort of misfeasance in public office.[314] This would be exacerbated by evidence of corrupt or improper motives.[315] Such consequences would be in addition to any proceedings following a complaint under the Privacy Act 1993. However, Todd and others argue that "legitimate public concern" may provide a defence to any legal action against a state agency or its officials.[316]

The state must restrain its own power in order to maintain the trust and confidence of the community. In 1998 the State Services Commissioner, Michael Wintringham, summarised the obligation that the state owes its citizens in respect of their personal information, which equally applies to non-citizens and businesses, as follows:[317]

> Citizens must have confidence that the information they provide to Government departments is treated carefully. This is the more so because citizens are compelled by law to provide certain information to the Government. In other words, there is an implicit compact between the State and citizen that, where the State exercises its power to collect information, it has an obligation to treat that information carefully.

The phrase "treated carefully" in the quote above implies controls over the way information is handled and shared. Accordingly, the proposed legal framework must have terms for protecting personal information and those terms must be transparent to ensure public confidence is maintained. In this regard, the New Zealand Law Society stated:[318]

> It appears… that Customs wishes to maintain public trust and confidence, but also wants significantly greater powers to share information with enforcement

---

[312] Crimes Act 1961 (New Zealand), ss 78 and 105A.

[313] Customs and Excise Act 1996 (New Zealand), s 182.

[314] *Three Rivers District Council v Governor and Company of the Bank of England* [2001] UKHL 16, (2001) 3 LGLR 36, [2001] 2 All ER 513, [2003] 2 AC 1, [2001] Lloyds Rep Bank 125, [2001] Lloyd's Rep Bank 125.

[315] *Garrett v Attorney-General* [1997] 2 NZLR 332 (CA).

[316] Stephen Todd, Cynthia Hawes, Bill Atkin, Ursula Cheer and John Burrows *The Law of Torts in New Zealand* (6th ed, Thomson Reuters, Wellington, 2013) 377, at 974.

[317] State Services Commission "Personal Information Protection and Public Confidence: State Services Commissioner's Overview" (22 December 1998) State Services Commission <ssc.govt.nz>.

[318] New Zealand Law Society "LawTalk Issue 866: More Detail Needed to Support Access to Customs Information" (5 June 2015) New Zealand Law Society <www.lawsociety.co.nz>.

> agencies, particularly the Police. …. However, without more detail … it is difficult to assess the potential privacy risks and harm posed by the proposals.

From the discussion above, it is evident that the protection of the right to privacy is important to the interests of the both the state and the public. It is important to include transparent privacy protection in the legal framework to improve public confidence in customs intelligence-sharing processes. The meaning of the right to privacy is discussed in more detail in Part VI below.

## *VI Privacy and the Secrecy of Personal Information*

This Part discusses the meaning of the right to privacy and introduces a model that aids the understanding of how abuses of the right in the practice of intelligence-sharing can harm the individual. The discussion provides some insight into the key issues that are relevant to the legal framework. It does not undertake a thorough examination of the concepts and meaning of privacy.

### *A The Right to Privacy*

The concepts of privacy and privacy protection are discussed in this sub-Part. The proposed legal framework enables personal information to be shared between the customs administrations of two or more states. Consequently, the right to privacy is affected. Secrecy about the existence and use of personal information also undermines an individual's right of access to justice. An individual cannot challenge the accuracy of personal information or defend themselves against its use, if they are unaware of the fact that it is being held.

The meaning of privacy can be unclear.[319] For example, it might involve trespass or a breach of confidence. The privacy impacts of electronic storage and of electronical information-sharing are widely debated.[320] The ambiguity has led some legislatures to adopt privacy principles as the parameters of privacy, such as New Zealand's Privacy Act 1993, rather than providing a precise definition that clarifies exactly what is meant by privacy.[321] To the casual observer, privacy law seems to be primarily focussed on the control and misuse of private information.[322] However, it is useful to understand the

[319] Ruth E Gavison "Privacy and the Limits of the Law" (1980) 89(3) Yale LJ 421, at 422 and Daniel J Solove "A Taxonomy of Privacy" (2006) 154 (3) Univ Penn Law Rev 477, at 478.

[320] Nicole Moreham "Privacy in the Common Law: a Doctrinal and Theoretical Analysis" (2005) 121 LQR 628, at 628 and Marc Rotenberg, Julie Horwitz and Jeramie Scott *Privacy in the Modern Age: The Search for Solutions* (The New Press, New York, 2015), at vii.

[321] At 5 for example.

[322] Nicole Moreham "Beyond Information: Physical Privacy in English Law" (2014) 73(2) CLJ 350, at 350.

origins of the term privacy.[323] Contemplating those origins aids the understanding of what is meant by privacy and the extent to which the proposed legal framework affects, or can protect, that privacy.

Privacy is originally a Western concept, developed under Roman law. The word "private" and the concept of privacy are used to make a person distinct from a group. For example, the term "private individual" is often used to designate a unique person acting with autonomy or in their own capacity.[324]

The abstract concepts of individual personality and autonomy were recognised in, and form the basis of, Roman law. In Roman law, individual personality was protected through the *actio iniuriarum*, which provided an action against harm to an individual's body, dignity or reputation.[325] The distinction of the individual as separate from the state is the foundation of Roman citizenship. The *civitas romana*, the body of Roman citizenship, is comprised of individual citizens who are distinct and can act autonomously of the whole state.[326]

Thus, the root purposes of privacy in Roman law were to preserve the ability to act autonomously from the state, to preserve individual personality and to protect the individual from harm to their body, dignity and reputation. Possession of private property is an expression of personality and, in some cases, it is a safe haven within which an individual can act freely and without fear of public scrutiny.[327] However, under Roman law the safe haven of private property was not immune from invasion by another to search for, for example, stolen property.[328]

The word "private" is used in the context of physical possessions, for example the phrase "private property" is used to convey ownership or possession of property by another, or others.[329] It is also applied in a more abstract sense to information. Information that is

[323] Jack Hirshleifer "Privacy: Its Origin, Function and Future" (the Economics and the Law of Privacy conference, University of Chicago, 30 November 1979), at 2.

[324] For example, in legislation such as Customs and Excise Act 1996 (New Zealand), at Schedule 1; Trustee Companies Act 1967 (New Zealand), at s 4(1); Larry W Beeferman *Images of the Citizen and the State: Resolving the Paradox of Public and Private Power in Constitutional Law* (University Press of America, Lanham, MA, 1996), at 373; and in commercial contexts such as Musees de grasse "You Are A Private Individual" (2017) Musees de grasse <www.museesdegrasse.com>.

[325] Bernardo Perinan "The Origin of Privacy as a Legal value: A Reflection on Roman and English Law" (2012) 52(2) American Journal of Legal History 183, at 190.

[326] At 195.

[327] At 189.

[328] T Lambert Mears (translator) *The Institutes of Gaius and Justinian, the Twelve Tables, and the CXVIIIth and CXXVIIth Novels* (Stevens and Sons, London, 1882), Gaius III ss 186, 187 and 191-193, at 492-493.

[329] Hirshleifer, above n 323 at 3.

regarded as private is deemed to be either information that is in the possession or control of an individual (inferring a property right), or information that is personal. The latter includes information that could potentially be used to identify an individual.

In regard to information, privacy is often equated to secrecy because both words involve the idea of controlled access.[330] Privacy in respect of private property like a house means the ability to control or to deny access by others. Likewise, some writers argue that privacy in respect of private information means the ability to control or deny access by others.[331] This information control definition of privacy is wrong, argues Parent, because when an information subject shares personal information with a friend, the subject gives up their privacy, but does not give up their control.[332] However, Moore points out that Parent confuses the right to privacy with the condition of privacy.[333]

The individual's grant of consent to the collection or use of their personal information is an act of autonomy.[334] The absence of an individual's consent when their personal information is secretly collected and used by governments erodes that autonomy. Governments deprive the individual of an opportunity to act when they neither provide the individual with an opportunity to sanction the collection of personal information, nor inform them of the purposes for which the information will be used.[335] Secret collection and use of information by governments can have "chilling effects on civic

[330] Carol Warren and Barbara Laslett "Privacy and Secrecy: A Conceptual Comparison" (July 1977) 33(3) Journal of Social Issues 43, at 43.

[331] A number of theorists support this view. See Charles Fried *An Anatomy of Values* (Harvard University Press, Cambridge MA, 1970), at 141;Charles Fried "Privacy" (1968) 77(3) Yale LJ 475; Moreham, above n 320, at 639; Irwin Altman "Privacy: A Conceptual Analysis" (1976) 8(1) Environment and Behavior 7, at 8;Irwin Altman "Privacy Regulation: Culturally Universal or Culturally Specific?" (1977) 33(3) Journal of Social Issues 66, at 68, and Gavison, above n 319, at 423. Gavison argues that privacy relates "to our concern over our accessibility to others". Other writers argue that privacy involves control of the information that would enable that accessibility. For other examples, see Christopher Hoadley, Heng Xu, Joey J Lee and Mary Beth Rosson "Privacy as Information Access and Illusory Control: The case of the Facebook News Feed Privacy Outcry" (2010) 9 Electronic Commerce Research and Applications 50, at 55 and Adam D Moore "Privacy: Its Meaning and Value" (2003) 40(3) American Philosophical Quarterly 215, at 218.

[332] W A Parent "Privacy, Morality and the law" (1983) 12 Philosophy and Public Affairs 269, at 273.

[333] Moore, above n 331, at 216. See also Parent, above n 332, at 269, in which the definition begins "Privacy is the condition of …".

[334] See Daniel R Ortiz "Privacy, Autonomy and Consent" (1989) 12 Harv JL & Pub Pol'y 91, at 92 and Daniel J Solove "Introduction: Privacy, Self Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880, at 1880.

[335] Rob Kitchin *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences* (Sage Publications, London, 2014), at 178.

participation".[336] Whether those instances of deprived autonomy lead to further harm to the individual is dependent on the subsequent uses and disclosure to which that information is put.

Modern privacy laws focus on the control of information.[337] This is despite the wording of the UDHR and ICCPR privacy articles, which do not deal explicitly with the notion of private or personal information:[338]

> No one shall be subjected to arbitrary [or unlawful] interference with his privacy, family, home or correspondence, nor [to unlawful] attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Although the word "correspondence" in the privacy articles relates to information, the words "family", "home", "honour" and "reputation" hark back to the Roman law concepts of the individual's body, dignity or reputation.[339]

Nonetheless, the link between the control of information in modern privacy laws and individual autonomy is apparent when one considers the effect of appropriating the identity of an individual, "Joe", for use in, say, advertising. Appropriating Joe's identity in that way could have a chilling effect on Joe's ability to move or interact with others in a public setting. Information can also be used in other ways to intentionally affect autonomy. For example, the online collection of an individual's viewing preferences and personal choices has been used by the Facebook web service to tailor the news and advertising shown to the individual.[340] That targeted news and advertising tends to lead the individual to hold certain opinions and make particular choices. That kind of manipulation limits the individual's knowledge and freedom of choice and it happens in a way over which the individual can exert no control.

Existing privacy laws focus on the control of information and enable an individual to maintain the integrity of, and a degree of secrecy for, their private information. The

---

[336] Deborah Hurley "Taking the Long Way Home: The Human Right of Privacy" in Marc Rotenberg, Julia Horowitz and Jeramie Scott *Privacy in the Modern Age: the Search for Solutions* (The New Press, New York, 2015) 70, at 75.

[337] For example, Privacy Act 1993 (New Zealand); Privacy Act 1988 (Australia); Privacy Act 1983 (Canada); Directive 2002/58/EC on Privacy in the Electronic Communications Sector [2002] OJ L201/37; Privacy and Electronic Communications (EC Directive) Regulations 2003 (United Kingdom); Personal Data (Privacy) Ordinance 2013 (Hong Kong); and Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Australia).

[338] UDHR, above n 234 at art 12 and ICCPR, above n 235 at art 17. The words "[or unlawful]" in the quotation above are words in the ICCPR article that do not exist in the UDHR article.

[339] Perinan, above n 325.

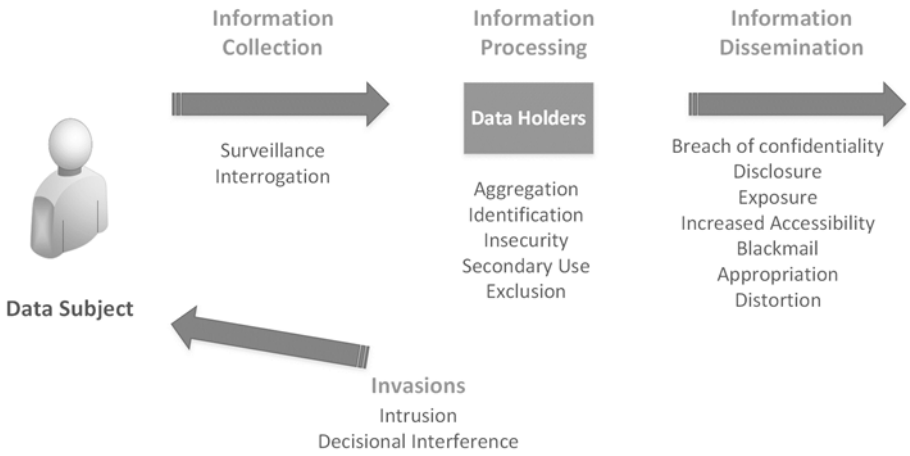
[340] Frank Pasquale "Privacy, Autonomy and Internet Platforms" in Marc Rotenburg, Julia Horowitz and Jeramie Scott *Privacy in the Modern Age: the Search for Solutions* (The New Press, New York, 2015) 165, at 165.

proposed legal framework enables customs intelligence-sharing with controls that help to maintain the integrity and secrecy for private information.[341]

### *B Activities that Harm Privacy*

This sub-Part examines the effect of implementing the principles of information privacy (hereafter, privacy) laws in a legal framework for customs intelligence-sharing. It discusses a model devised by Daniel Solove which describes groups of activities that are harmful to privacy. [342] This model is useful to understand privacy violations in the customs intelligence-sharing context. Figure 8 illustrates Solove's taxonomy of privacy.

**Figure 8. Solove's taxonomy of privacy**



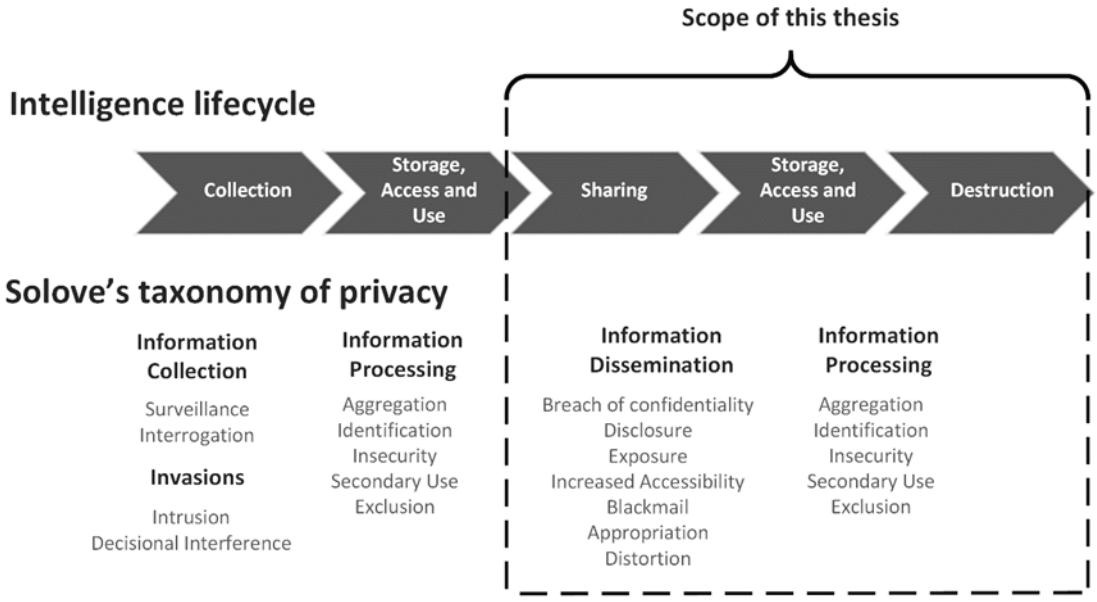

Solove's taxonomy of activities that harm privacy is a model that is defined in four basic groups of activities: information collection, information processing, information dissemination and invasion. The harmful activities that need to be addressed for present purposes are within the information dissemination and information processing groups. This is because the scope of the legal framework is the sharing and further use of information that has previously been obtained and used by a customs administration.

Solove's model can be mapped to the intelligence-sharing lifecycle shown in Figure 9.

[341] Other laws may exist that relate to state interference in the home, family, autonomy and other aspects of an individual's privacy. An analysis of those laws is outside the scope of this work on customs information-sharing.

[342] Solove, above n 319, at 489–549.

**Figure 9. Solove's taxonomy within the intelligence lifecycle**




The information processing harms that are the most relevant to the proposed legal framework are Aggregation, Insecurity, Secondary Use and Exclusion. The information dissemination harms that are the most relevant are Breach of Confidentiality, Disclosure, Exposure and Increased Accessibility. The harms of the least relevance are the information collection and invasion groups of harms, the information dissemination harms of Blackmail, Appropriation and Distortion, and the information processing harm of Identification.

The harms are addressed through the implementation of privacy principles in the legal framework. There is not a one-to-one match between each harm, as described by Solove, and the coverage of a privacy principle. However, the privacy principles that provide the most protection from Solove's harms are Purpose Specification, Use Limitation, Data Quality and Security Safeguards. The privacy principles are discussed in more detail in Chapter Four. The implementation of the privacy principles is discussed in Chapter Six and Chapter Seven.

Each of the groups of harmful activities from Solove's taxonomy are briefly described as follows.

### *1 Information collection*

During information collection, harm can occur through surveillance, which is "watching, listening to, or recording an individual's activities".[343] Greenwald describes privacy from surveillance as "a core condition of being a free person".[344] The second activity in this

[343] At 493.

[344] Greenwald, above n 143, at 172.

group is interrogation which comprises questioning or probing for information. These activities have an obvious effect in the context of information secrecy. They can affect the autonomy of the individual by creating feelings of anxiety and discomfort and lead the individual to change their behaviour.[345] These behavioural changes may be unwanted by individuals, but they can be advantageous to customs administrations if those changes lead to increased compliance with customs law. The information used by customs processes that has been gathered through customs and other government agency paperwork can be thought of as gathered through a form of interrogation. Customs information collection activities are not within the scope of the proposed legal framework, as the method of initial collection is not integral to information-sharing processes.[346]

*2 Invasions*

Solove describes two types of invasions that can harm privacy: Intrusion, which involves the invasive acts that interfere with the individual's tranquillity and solitude; or Decisional Interference which is the government's intrusion into the individual's decisions regarding their private life.[347] The proposed legal framework addresses the processes used by customs administrations to share information with other customs administrations. It is not aimed at direct and unsolicited engagement with any individual. Downstream activities such as conducting a search or making an arrest would involve these invasions described by Solove, but those activities are outside the scope of the information-sharing processes.

*3 Information processing*

Five potentially harmful information processing activities are described by Solove: Aggregation, Identification, Insecurity, Secondary Use and Exclusion.[348]

(a) Aggregation

The first potentially harmful activity, aggregation, already occurs in customs risk-management processes. Chapter Two described how customs administrations collect information about the entities involved in a trade transaction, aggregate and analyse the information to assess the risk of non-compliance with customs law. Aggregation involves the combination of various pieces of information about an individual. This activity is

[345] Ibid.

[346] Although an intelligence source may impose rules on the subsequent sharing and use of information it supplies.

[347] Solove, above n 319, at 491.

[348] At 490.

central to the proposed legal framework as aggregated information is used in intelligence processes to assess the risk presented by an individual.[349] Solove argues:[350]

> …aggregation can cause dignity harms because it unsettles expectations. People expect certain limits on what is known about them and what people will find out.

Customs data aggregation can include all the historical transactions in which the entities were involved. The historical transactions can reveal patterns of behaviour and the identification of unusual transactions with unusual characteristics. The extent to which this aggregation causes dignity harm, as described by Solove, is difficult to assess and is possibly an area for further research. Aggregation can lead to Big Data, which means data held in such large amounts that it can be difficult to process.[351] Big Data potentially creates policy challenges about balancing privacy needs against national security and law enforcement needs.[352] There is public expectation that governments collect and analyse information to prevent security risks and other crime. In New Zealand, the customs intelligence processing capability is enabled by publicly accessible legislation and the capability is advertised on its website.[353] The legal framework advocated here includes controls that require regular checks so that information is destroyed when it is no longer needed. These controls might reduce the public concern regarding aggregation. The final and most important factor reducing the harm of aggregation is that the proposed approach does not include a centralised, aggregated database that can be accessed by all customs administrations. Instead, it proposes the automation of manual intelligence-sharing practices that already exist. Each customs administration would continue to maintain its own intelligence repository, separate from the information collections of all other customs administrations.

(b) Identification

The second potentially harmful information processing activity is identification, which

[349] Colleen McCue *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis* (2nd ed, Butterworth-Hienemann, Oxford, 2015), at xxiii and 3.

[350] Solove, above n 319, at 508.

[351] Dictionary.com "Big Data" (2017) Dictionary.com <www.dictionary.com>. Big Data is discussed in Chapter Four.

[352] Christopher Wolf and Marc Rotenberg "Envisioning Privacy in the World of Big Data" in Julia Horwitz and Jeramie Scott *Privacy in the Modern Age: the Search for Solutions* (The New Press, New York, 2015) 204, at 205, and Jules Polonetsky, Omer Tene and Christopher Wolf "How to Solve the President's Big Data Challenge" (2014) The International Association of Privacy Professionals <www.iapp.org>.

[353] Customs and Excise Act 1996 (New Zealand), ss 38A–38Q, 281, 282 and 282A–282L. See also New Zealand Customs Service "Intelligence-led" (2017) New Zealand Customs Service <www.customs.govt.nz>.

means the association of data with a particular individual.[354] Identification may harm an individual because it attaches informational "baggage" to an individual about past behaviour.[355] However, this baggage is essential to customs risk-management as it provides powerful indicators of possible future behaviour, especially as a small number of recidivists commits a disproportionately large amount of crime.[356] A central argument against the identification harm is its effect on autonomy as it "inhibits people's ability to change and it can prevent their self-development by tying them to a past from which they want to escape".[357] In the customs risk-management context, identifying the individual does not in any way inhibit them from making legitimate transactions. In fact, any legitimate transactions made by the individual will be a matter of record. The only antidote to the harm caused by identification in this context is for customs to treat every individual as an anonymous person, which would inhibit much of the risk-management process. Identification harm is unavoidable in this context.

(c) Insecurity

The third harmful activity described in Solove's model, insecurity, occurs when information is stolen and used for other purposes, such as identity theft.[358] Security of information is central to any intelligence and law enforcement process because it affects the security of current and future operations and the trust afforded by the sources of intelligence.[359] Security of information is also essential to public trust in government as a whole. The proposed legal framework addresses the risk of insecurity by suggesting controls that ensure information is protected and the ongoing security of information is assured before it is shared with another customs administration.

(d) Secondary use

The fourth potentially harmful activity is secondary use, which means the use of information for purposes other than for which it was collected. This causes harm to dignity as "it involves using information in ways to which a person does not consent and might not find desirable".[360] Information such as airline passenger information is used

[354] Solove, above n 319, at 511.

[355] At 513.

[356] Jerry Ratcliffe "Intelligence-led Policing" (2003) April(248) Trends and Issues in Crime and Criminal Justice 1, at 2 – 3.

[357] Solove, above n 319, at 514.

[358] At 516.

[359] *Snepp v United States* 444 US 507 (1980), at 512 and 513.

[360] Solove, above n 319, at 521.

for secondary purposes in customs risk-management processes.[361] Like the harm of aggregation, the harm caused by secondary use is partially mitigated by the public expectation that governments collect and analyse information in this way to address security risks and other crime. The proposed legal framework places restrictions on the use of information shared with other customs agencies to reduce the potential for harm through use for secondary purposes other than customs purposes.

(e) Exclusion

The fifth information processing harm described by Solove is exclusion. The exclusion harm occurs when an individual is unable to find out what information is held about themselves and how it is used.[362] Further harm is caused when the individual is unable to correct inaccurate information held about them. The exclusion risk is amplified in existing customs information-sharing arrangements. Individuals are unable to know with what customs administrations their information has been shared. Furthermore, there are no facilities in place that enable individuals to correct inaccurate information held by any customs administration. The existence of incorrect information, or the individual's knowledge of it, may result in particular actions by the customs administration or behavioural changes in the individual, which would infringe the individual's autonomy.[363] The controls suggested in the proposed legal framework would require inaccurate information to be corrected quickly by any party in possession of that information.

*4 Information dissemination*

The dissemination, or sharing, of information is at the heart of the proposed legal framework. Solove describes seven information dissemination activities that can harm privacy. These are: breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion.[364] These potentially harmful activities are discussed below.

(a) Breach of confidentiality

The first potential harm from dissemination, breach of confidentiality, damages relationships built on trust.[365] A breach of confidentiality damages the trust that the

[361] Customs and Excise Act 1996 (New Zealand), s 38E.

[362] Solove, above n 319, at 523.

[363] For example, a customs administration may delay a trader's goods transaction in order to conduct an inspection, or a trader might take additional steps or avoid certain types of business if they know the customs administration has particular information about them.

[364] Solove, above n 319, at 525.

[365] At 526.

individual has placed in the person to whom, or organisation to which, it has entrusted information. Consequently, the tort of breach of confidentiality in the United States focuses on the content of the breach, rather than the source of the breach, where the disclosure is neither compelled by law nor by the consent of the data subject.[366] In New Zealand, the breach of confidentiality is made lawful in the customs context through legislation.[367] Nonetheless and regardless of whether the individual is aware of the legislation that enables it, an individual may lose trust in the party to which it has provided information. This harm is unavoidable if customs administrations are to collect, evaluate and use personal information in risk-management processes.

(b) Disclosure

The potential harms that result from disclosure are the second group of information dissemination harms described by Solove.[368] Disclosure can threaten an individual's safety, for example when the identity of the carrier of high-value goods is discovered by a criminal. Disclosure can also threaten financial security, for example when the sale price of imported or exported goods is disclosed to a competitor.

Disclosure can also cause dignity harm, for example when information that an individual would prefer to remain secret and which causes reputational damage is disclosed. Disclosure harms are mainly harms resulting from public release. In the customs information-sharing context, a form of reputational harm can occur when information about a trader's past activities is revealed. For example, a customs administration might harm the reputation of a trader if it discloses that trader's history of non-compliance with customs laws to another customs administration. However, that reputational damage involves only the regard of the trader by the customs administrations unless the information is publicly disclosed. The proposed legal framework aims to protect private information from public disclosure, unless it is required to be presented to the court in a prosecution.

(c) Exposure

The third source of harms in Solove's model is exposure. Exposure is the disclosure of information or activities to one or more others which would constitute a gross invasion of the individual's privacy. It involves physical and emotional attributes and personal behaviour which can cause acute embarrassment and humiliation if revealed and which are "… not revealing of anything we typically use to judge people's character".[369] Harm from exposure occurs because societal norms obscure personal traits and activities for

[366] Ibid and *McCormick v England* 494 SE 2d 431, 432 (SC Ct App 1997).

[367] For example, for passenger information, Customs and Excise Act 1996 (New Zealand), s 38E.

[368] Solove, above n 319, at 531-533.

[369] At 536.

reasons of decency. Harm from exposure in the customs information-sharing context of the proposed legal framework is unlikely because:

1. this information is by definition not information that is typically used by customs administrations to judge people's character, so it is unlikely to have been collected by customs; and
2. the situations in which customs administrations collect and hold this information are specific to legal offences against decency such as the importation or distribution of offensive material; and
3. the individual is shielded from humiliation and embarrassment by controls that protect information from public disclosure, except in legal proceedings.

(d) Accessibility

Solove describes increased accessibility as a fourth potential source of privacy harms. Increased accessibility, in Solove's description, means information which may have been available to the public is made more easily accessible.[370] For example, information about land or vehicle ownership is placed online. The harm that can occur as a result of increased accessibility includes commercial use of information that was previously difficult to access for targeted marketing and profiling.[371] This is exactly what happened in the United Kingdom when the Metropolitan Police made the details of 30,000 London gun owners available to a direct marketing agency.[372] The harm from increased accessibility is prevented by controls in the proposed legal framework which allow only government access to the shared information.

(e) Blackmail

Blackmail is the fifth potential harm that Solove believes can arise from information dissemination. Individuals can suffer harm through the public exposure of information or the disclosure of information to specific others. Blackmailers who possess or who can access information that would damage the reputation or dignity of an individual may threaten to expose that information unless the individual makes a payment or performs an act that the blackmailer demands. Coercion of this type could be done by a customs officer who has access to any damaging information that is exchanged through the proposed legal framework. The individual is protected from this kind of blackmail by

[370] At 540.

[371] Daniel J Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2006), at 131 and Robert Gellman "Public Records, Public Policy, and Privacy" (1999) 26(1) Human Rights 7, at 7.

[372] Gareth Corfield "30,000 London Gun Owners Hit by Met Police 'Data Breach'" (2017) The Register <www.theregister.co.uk>.

controls that prevent access and use for non-customs purposes, and more generally by domestic laws against blackmail.[373]

(f) Appropriation

Appropriation, or the use of someone's likeness by another, is the sixth possible source harm that can arise from information dissemination.[374] Appropriation can cause harm to an individual's dignity and reputation. In cases of identity theft and fraud, appropriation is a criminal offence.[375] Appropriation is not likely to be purposely done by a customs administration. It is self-evident that accuracy of the identity of an individual is crucial to the risk-management of the individual's transactions by customs. However, there is a risk that an identity will be mistakenly attributed to an individual. Such a mistake might result in unnecessary intervention or further investigation by a customs administration. For this reason, controls are included in the legal framework to ensure shared information is accurate and is kept up to date.

(g) Distortion

The seventh and final source of harm through information dissemination is distortion. Distortion is the misrepresentation or falsification of information to injure a person's reputation.[376] Harm from distortion occurs when libellous or slanderous information is disseminated. Defamation law exists to protect the individual from such harm.[377] Distortion is unlikely to create harm to an individual through the use of the approach advocated here. It is because the framework has controls to prevent information from being revealed publicly and the risk-management processes used by customs rely upon accurate and up to date information. Nonetheless, inaccurate information could lead to unnecessary interventions, such as searches, and investigations of the individual. To reduce the risk of these unnecessary interventions and investigations, controls exist in the legal framework to ensure information remains accurate and up to date and inaccurate information is quickly identified and set aside.

## *VII Chapter Summary*

With an appropriate legal framework, the customs single window could be used to automate intelligence exchanges. This Chapter supports the thesis by describing the rights that should be protected in the proposed legal framework.

---

[373] For example, Crimes Act 1961 (New Zealand), s 237.

[374] Solove, above n 319, at 546.

[375] For example, Crimes Act 1961 (New Zealand), ss 240 and 259.

[376] Solove, above n 319, at 549.

[377] Todd et al, above n 316, at 809 – 931.

The proposed legal framework shows that intelligence-sharing agreements can include transparent protection for human rights. One that does make the protection of these rights evident has a better prospect of public acceptance than methods that do not contain that protection.

This Chapter provided an overview of the human rights which, if prudently treated, should lead to improved public confidence in customs intelligence-sharing. This research did not propose a framework for human rights. Other international instruments and organisations exist for that purpose. The UN instruments for human rights were accepted as benchmarks for their treatment. No normative claims were made about the value of these human rights or the manner in which they are expressed.

The human rights that are most likely to be directly or indirectly affected by the sharing of customs intelligence through a single window system are the rights of access to justice, freedom from arbitrary search and seizure, freedom from torture and privacy. Privacy was identified as the human right most directly affected by customs intelligence-sharing. Other human rights are only indirectly affected.

The discussion suggested that the right to privacy encapsulates the need to protect the individual's autonomy and to protect them from harm to body, dignity and reputation. The right to privacy is a concern for the customs intelligence-sharing because it entails the sharing of personal information.

Solove's taxonomy of privacy was provided as a useful model to help understand the breadth of privacy harms that can occur through the collection, handling, use and sharing of personal information by customs administrations. The principles in privacy legislation help to protect the individual from the harms described by Solove. However, the secrecy of information in government intelligence processes and the privacy exemptions that governments provide to intelligence processes impede the protection of the privacy. The proposed legal framework does not improve every aspect of information privacy in intelligence processes, but the potential for the harms described by Solove is reduced by implementing the privacy principles.

The next Chapter discusses existing privacy law and identifies the privacy principles that can be implemented in the legal framework within practical limits in order to improve trust and confidence. The ability of the public to scrutinise and debate the treatment of privacy in intelligence-sharing agreements should improve public confidence in the operation of customs administrations.

# Chapter Four – Establishing a Benchmark for Transparent Privacy

Chapter Three identified secrecy about the treatment of human rights as an impediment to public confidence in government exchanges of personal information. It explained that privacy is most often considered in relation to personal information in modern contexts. Information privacy is the human right most affected by customs intelligence-sharing as it involves personal information. The misuse of personal information has the potential to cause other human rights abuses. Therefore, clear terms that protect privacy will enhance public confidence in this proposed legal framework.

This Chapter focuses on the right to privacy. It has eight Parts. Part I discusses the increasing governmental use of technology and large collections of personal information. This increased use of technology has led to public debate about the use of Big Data and its effect on privacy. Part II tells how this risk and concern has been compounded by changing uses of information and the changing public attitudes following the 9/11 terrorist attacks. It considers some Big Data issues that need to be addressed by the model for sharing intelligence through a single window system. Part III discusses the effect of Edward Snowden's disclosure of classified intelligence information on public expectations for the treatment of privacy. This discussion emphasises the changing public expectations regarding the treatment of privacy and the use of Big Data in the intelligence and law enforcement contexts.

The evolving body of tort law and legislation is considered in Part IV and Part V to provide more background to the requirements for privacy protection. Part VI identifies the commonly accepted Privacy Principles in international legislation and they are transparently protected in the proposed legal framework. This transparency contributes to public confidence and addresses some of the concerns identified in Part I, Part II and Part III and in Chapter Three. Part VII relates those Privacy Principles to Solove's taxonomy of privacy model, which was introduced in Chapter Three. Part VII also discusses the limits of the comfort that individuals can draw from the treatment of privacy in the proposed legal framework. Part VIII summarises the findings of this Chapter.

## *I Privacy, Databases and Other Electronic Systems*

This Part explains how the increased use of technology by governments has amplified concern about secrecy and the risk to privacy. The legal framework proposed here supports the use of technology to exchange intelligence and other information. Some aggregation of data is inherent in the use of the system because customs administrations aggregate data for analysis in risk-assessment processes. Many of the privacy concerns associated with Big Data relate to sharing and using information for additional, often

unstated purposes. This discussion is only an overview. It is not a detailed analysis of the privacy issues associated with databases and Big Data. This Part explains why the proposed legal framework has controls to help prevent intelligence shared through a single window system from being used for non-customs purposes.

Concerns about government use of Big Data have been well documented. In his 2015 report to the United Kingdom Prime Minister on his review of investigatory powers, Anderson stated:[378]

> Bulk collection of both communications data and intercepted material has been one of the leading sources of controversy following the disclosure of the Snowden Documents.

Duncan commented specifically on the constraining effect of secrecy in the collection and use of large collections of personal information, stating:[379]

> Individual autonomy is the capacity of a person to function in society as an individual, uncoerced and cloaked by privacy. Individual autonomy is compromised by the excessive surveillance sometimes used to build databases; a lack of informed consent from subjects who are not told about the purpose, sponsorship, risks and benefits of voluntary research before deciding whether or not to participate; unwitting dispersion of data; and a willingness by those who collect data for administrative purposes to make them available in personally identifiable form.

State and commercial collections of information about individuals are not a recent development, but the use of technology to process Big Data is relatively novel.[380] The movements of all mobile phone users can be tracked and tied to other information, resulting in "ubiquitous data collection".[381] Harcourt notes that "commerce is collapsing into surveillance, right before our eyes, as retailers begin to collect all our data".[382] This

[378] Anderson, above n 201, at 78 para 5.31.

[379] Duncan, above n 225.

[380] United States President's Council of Advisors on Science and Technology *Report to the President - Big Data and Privacy: A Technological Perspective* (Office of the President of the United States, Washington DC, May 2014), at ix. See also Anderson, above n 201, at 49 paras 4.2– 4.6 and at 57 para 4.36.

[381] Christopher Kuner, Fred H Cate, Christopher Millard and Dan Jerker B Svantesson "The Challenge of 'Big Data' for Data Protection" (2012) 2(2) International Data Privacy Law 47, at 47. See also Lyon, above n 175, at 71.

[382] Bernard E Harcourt *Exposed: Desire and Disobedience in the Digital Age* (Harvard University Press, Cambridge MA, 2015), at 188 and Kitchin, above n 335, at 166–167.

increased use of technology to collect, share and process information has heightened the need for good privacy controls.[383]

For decades it has been recognised that controls are required to moderate the state's collection and use of such information because, without such controls, the individual's freedoms are constrained.

For example, Black J noted in *Baird v State Bar*:[384]

> … when a state attempts to make inquiries about a person's beliefs or associations, its power is limited by the First Amendment. Broad and sweeping state inquiries into these protected areas… discourage citizens from exercising rights protected by the Constitution.

During the 1980s, the United States Customs began to connect the electronic networks of all federal departments and agencies that had jurisdiction over international trade.[385] In 1989 the United States Supreme Court noted particular concerns in respect of computerised systems that store, summarise and share large quantities of personal information. In *DoJ v Reporters Committee for Freedom of the Press,* the court found: [386]

> Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerised summary located in a single clearinghouse of information.

The United States Treasury then began to build the International Trade Data System in 1994 and 53 government agencies participated in the detailed planning.[387]

Computerisation like this has raised fears for privacy and while technology may not have created privacy invasions, it may have aggravated existing threats. [388]

---

[383] For example, see Wilson, above n 11 and Solove, above n 319. See also, for example, Anderson, above n 201, at 14.89. See also Kuner et al, above n 381, at 48.

[384] *Baird v State Bar* 401 US 1 (1971).

[385] Jane Fountain *Building the Virtual State: Information Technology and Institutional Change* (Brookings Institution Press, Washington DC, 2001), at 117.

[386] *DoJ v Reporters Committee for Freedom of the Press* 489 US 749 (1989).

[387] Fountain, above n 385, at 126.

[388] Priscilla Regan *Legislating Privacy: Technology, Social Values and Public Policy* (2nd ed, University of North Carolina Press, Chapel Hill NC, 2009), at 11.

In 1998 the New Zealand Privacy Commissioner also recognised a general risk to privacy through the use of electronic systems and databases, saying in respect of health information systems:[389]

> I believe the Government faces considerable risks arising from the development of centralised databases, apart from the usual risks of such systems. The risk is that there has been little or no consumer consultation about the plans that are being made for the obtaining, use and disclosure of health information about identifiable individuals. These plans may well suit the needs of health funders, managers, economists, accounting and auditing professionals and may even accord with good medical practice. But if the people do not trust the system, they will rebel.

The New Zealand Law Commission noted:[390]

> Greater uptake of technological applications has reduced de facto privacy protections such as information being widely dispersed and difficult to access, and limitations on physical storage.

When inaccurate information is distributed to multiple databases, it becomes difficult to locate and correct.[391] The widespread distribution of data and subsequent data aggregation leads to data subjects losing knowledge and control of the downstream uses of their information.[392] Storing intelligence in a centralised pool also inhibits the timely deletion of intelligence when it is no longer required. This is because to delete the information, every party to the system would need to indicate that it no longer has a use for the information. Conversely, in a decentralised system such as the one envisaged for the legal framework, every party can delete its own copy of the information that it no longer requires. Also, when providing their personal information, individuals often fail to read or understand privacy policies which may rely on ambiguous language, making consent an "empty exercise".[393]

---

[389] Bruce Slane "Centralised Databases: People, Privacy and Planning - a Paper Presented by the Privacy Commissioner to the New Zealand - Australia Health IT Directors meeting" (18 February 1998) Privacy Commissioner <privacy.org.nz>.

[390] New Zealand Law Commission "Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4 (NZLC IP17)" (2010) New Zealand Law Commission <www.lawcom.govt.nz>, at 350.

[391] "Ministerial Briefing: Information Sharing" (2011) New Zealand Law Commission <www.lawcom.govt.nz>, at 5.

[392] Melissa De Zwart, Sal Humphries and Beatrix Van Dissel "Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK" (2014) 37(2) UNSWLJ 713, at 715. See also John Pavolotsky "Privacy in the Age of Big Data" (2013) 69(1) The Business Lawyer 217, at 220.

[393] Ira S Rubinstein "Big Data: The End of Privacy or a New Beginning?" (2012) 3(2) International Data Privacy Law 74, at 75, and Kitchen, above n 335, at 172.

Consequently, the New Zealand Law Commission recommended an accreditation system for authorising bulk access to public registers of information.[394]

For the reasons described in this Part, the proposed legal framework will not use a centralised database. Instead, it enables automated, state-to-state information-sharing on a case-by-case basis. This avoids the privacy risks associated with the on-sharing of Big Data and its re-use for other purposes, ensures that privacy principles are implemented effectively and supports customs risk-management processes with accurate and up-to-date information.

The alternative approach of pooling information in a central repository that is accessible by all the parties to an intelligence-sharing arrangement is impractical. Intelligence partnerships are founded on both trust and mistrust. Document markings of national caveats such as NZ/UK EYES ONLY or AUS/UK EYES ONLY are intended to restrict document access to personnel from specified states.[395] In the Five Eyes intelligence partnership some intelligence material is shared between only a subset of the Five Eyes partners.[396] It follows that a central pool of intelligence involving more than two parties could only be managed by a body that possesses all of required nationalities and none of the excluded nationalities for every item of intelligence. It is not possible to manage these competing needs with a centralised pool of customs intelligence shared through a single window system. Similarly, it is not practical to have a common and centralised compliance monitoring body.[397] While the method of state-to-state information-sharing on a case-by-case basis in the proposed legal framework will go some way towards allaying public concern, it is important to note that government and public attitudes toward governmental use of personal information changed after the 9/11 terrorist attacks. These changes are discussed in Part II, below.

## *II Changes since 11 September 2001*

Since the 9/11 terrorist attacks there has been increasing public scrutiny and media focus on governments' use of vested powers for intelligence and security. This Part provides an overview of those changes and the subsequent increased need for transparency in the proposed legal framework.

---

394 "Public Registers: Review of the Law of Privacy Stage 2 (NZLC R101)" (2008) New Zealand Law Commission <www.lawcom.govt.nz>, at [R9].

395 United Kingdom Cabinet Office "Government Security Classifications 2014" (2014) United Kingdom Cabinet Office <www.gov.uk>, at 12.

396 Ibid.

397 Accountability for compliance with the legal framework is discussed further in Part VI of this Chapter.

"The global war on terrorism" has given governments "greater latitude to disregard the constraints of human rights law and humanitarian law".[398] This "trade-off between security and civil liberties might represent a judgment that we fear our own government more than we fear terrorists", says Luban.[399] Luban's argument is that trading-off basic human rights for security is foolish because in the act of doing so, the state is deconstructing the society it is seeking to protect.

The United States government's focus for intelligence and security changed significantly after the 9/11 terrorist attacks. In this regard, Duncan noted:[400]

> Importantly, these events triggered a shift in national security thinking from how to deal with the threat from nation-states to how to deal with the threat from individuals and small groups. Dealing with such threats clearly requires data on individuals and their relationships, a much different imperative than seeking information on the Soviet Union's nuclear program.

Following a report issued by the National Commission on Terrorist Attacks Upon the United States, the United States government enacted legislation to create the role of Director of National Intelligence to overcome perceived intelligence failings.[401]

The Director of National Intelligence oversees the provision of intelligence to the President, oversees the budget of the National Intelligence Programme and leads the Joint Intelligence Community Council.[402] The legislation also set out the role of the Privacy and Civil Liberties Oversight Board to help oversee and protect human rights in intelligence activities.[403]

---

[398] Neil Hicks "The Impact of Counter Terror on the Promotion and Protection of Human Rights: A Global Perspective" in Richard Ashby Wilson *Human Rights in the War on Terror* (Cambridge University Press, Cambridge UK, 2006) 209, at 209.

[399] David Luban "Eight Fallacies about Liberty and Security" in Richard Ashby Wilson *Human Rights in the War on Terror* (Cambridge University Press, Cambridge UK, 2006) 242, at 245.

[400] George Duncan "Exploring the Tension Between Privacy and the Social Benefits of Governmental Databases" (the Security, Technology, and Privacy: Shaping a 21st Century Public Information Policy conference, 24-25 April 2003, Washington DC), at 12.

[401] Thomas H Kean, Lee H Hamilton, Richard Ben-Veniste Fred F Fielding and Others *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Government Printing Office, Washington DC, 2004), at 407, and 118 Stat 3638 Intelligence Reform and Terrorism Prevention Act 2004 (United States), s 1011.

[402] 118 Stat 3638 Intelligence Reform and Terrorism Prevention Act 2004 (United States), ss 1011, and 1031.

[403] Section 1061.

Since the 9/11 terrorist attacks a proportion of the United States public has been amenable to a limitation on the right to privacy. Bidgoli noted the public's attitude had polarised, saying: [404]

> After September 11 2001, many Americans have said they are willing to sacrifice some privacy to feel more secure, but to others the existence of government surveillance systems such as Carnivore and Echelon point to an Orwellian future.

One such example is Fisher's exposé on New Zealand Police use of the Privacy Act 1993 to obtain information from airlines, banks, electricity companies, internet providers and phone companies without a warrant.[405] Principle 11 of the Act states:[406]

> An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds ....
>
> ….
>
> (e) that non-compliance is necessary
>
> (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
>
> (ii) for the enforcement of a law imposing a pecuniary penalty; ….
>
> (iii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
>
> (f) that the disclosure of the information is necessary to prevent or lessen a serious threat (as defined in section 2(1)) to –
>
> (i) public health or public safety;
>
> ….

Fisher claimed that the New Zealand Privacy Commissioner was concerned about the practice, which increasingly sees companies voluntarily give information without the compulsion of a warrant.[407] The New Zealand Police had not recorded the number of such requests it had made. [408] Jonathan Eaton QC said there "was a burden of

[404] Hossein Bidgoli (ed) *Global Perspectives in Information Security* (Wiley & Sons, New Jersey, 2004).

[405] David Fisher "Police Exploiting Privacy Act" *The New Zealand Herald* (Auckland, 25 March 2015), at A10.

[406] Section 6.

[407] Fisher, above n 405.

[408] Ibid.

transparency on companies that hold personal information" and an obligation to inform their customers when their information was disclosed to the Police.[409]

The United States is now changing its intelligence operations in response to public concern about the widespread interception and use of personal communications since the 9/11 terrorist attacks.[410]

Other events, both domestically and internationally, have highlighted that the attitude of the New Zealand public to privacy, intelligence and security has changed in a similar way. For example, in 2015 the Inspector General of Security investigated the GCSB's interpretation of "private information" in the GCSB Act.[411] The GCSB is the intelligence agency tasked with gathering intelligence from foreign communications and computing systems.[412] A media report at that time had claimed revelations about spying meant that the public increasingly expected their communications to be intercepted. It was alleged that this in turn gave GCSB more freedom to intercept the communications of New Zealanders.[413] This is because, although the GCSB Act prohibited the interception of the private communications of New Zealanders, it also states that "private communication":[414]

> … does not include a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so.

If the GCSB used a generous interpretation of "private communication", it may not have done so with ill intent. It is possible that the GCSB officials believed that they acted with integrity and good intention.

Governments took greater latitude to disregard human rights in their response to terrorist threats following the 9/11 terrorist attacks. Since then, public opinion of government integrity has been guided by media reports that argue that government agencies should

---

[409] Ibid.

[410] As evidenced by USA Freedom Act 50 USC § 1862 (United States) and as discussed in Editorial "A New Age of Espionage; Intelligence and Democracy" *The Economist* (online edition, London, 1 August 2015) at 53-54.

[411] Brent Edwards "Spy Watchdog to Investigate GCSB" (31 March 2015) Radio New Zealand News <www.radionz.co.nz> and GCSB Act. The outcome of that investigation was not publicly reported.

[412] GCSB Act, above n 176, ss 8A, 8B and 15A.

[413] Dennis Tegg "Loophole that Legalises Official Snooping" *The New Zealand Herald* (online edition, Auckland, 15 August 2014).

[414] GCSB Act, above n 176, ss 4 and 14(1).

be transparent in their compliance with both the letter and intent of the law.[415] Such publicity has led to privacy reforms.[416] The Snowden leaks have resulted in intense public debate and resulted in significant changes in public attitudes and government practices. Greater transparency for privacy controls is needed to ensure on-going public confidence in the integrity of government.

The discussion in Part III focusses on the Snowden Leaks, the resulting publicity and change in government intelligence practices and its implications for customs intelligence-sharing through a single window system.

## *III The Snowden Leaks*

In June 2013, *The Guardian* began publishing revelations from 58,000 previously secret NSA documents leaked by Edward Snowden.[417] The Snowden leaks have sparked widespread debate about government surveillance and use of personal information.[418] One issue of particular concern has been the collection, storage and data-mining of vast amounts of metadata to track people's online and telephone communications.[419] This Big Data intelligence information is presumably available to the NSA's partner agencies in the Five Eyes intelligence partnership.[420] The Snowden revelations generated public debate and resulted in heightened public distrust of secret intelligence activities.[421] At the same time, governments have been criminalising investigative journalists and treating

[415] For other examples, see Andrew Sparrow "Intelligence Committee Publishes its Report on Privacy and Security: Politics Live Blog" *The Guardian* (online edition, London, 12 March 2015); "Intelligence Agencies Demand 'Blanket Exemption' from Right to Privacy Bill" *The Economic Times* (online edition, Delhi, 2015); Andy Greenberg "Privacy Critics go 0-2 with Congress' Cybersecurity Bills" (26 March 2015) Wired <www.wired.com> and Griffith, above n 215.

[416] Benjamin Goold and Daniel Neyland *New Directions in Surveillance Privacy* (Routledge, London, 2013), at 5. See also Peter Gill *Policing Politics: Security Intelligence and the Liberal Democratic State* (Frank Cass, London, 1994), at 300 and Loch K Johnson *A Season of Inquiry: The Senate Intelligence Investigations* (The University Press of Kentucky, Lexington, 1985), at 27.

[417] Mirren Gidda "Edward Snowden and the NSA files – Timeline" *The Guardian* (online edition, London, 22 June 2013) and Lyon, above n 175, at 1.

[418] Emily Berman "Quasi-Constitutional Protections and Government Surveillance" (2016) 3 BYU L Rev 771, at 773.

[419] At 775 and 776, and Leah Angela Robis "When Does Public Interest Justify Government Interference and Surveillance?" (2014) 15 Asia-Pacific Journal on Human Rights and the Law 203, at 204.

[420] Patman and Southgate, above n 176, at 874 and Lyon, above n 175, at 8.

[421] Patman and Southgate, above n 176, at 875 and Rachel Levinson Waldman "Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public" (2017) 66(3) Emory LJ 527, at 554.

them as a threat to security "whose activities are to be guarded against in the same way as foreign intelligence services and subversive or terrorist organizations".[422]

Greenwald likened the Snowden revelations to the covert FBI surveillance and counter-protest activity in the 1970s.[423] A United States Senate report declared that activity "unworthy of a democracy and occasionally reminiscent of totalitarian regimes".[424]

There have been other leaks of intelligence methods and material. For example, the WikiLeaks website first began publishing secret intelligence material and techniques in 2006.[425] Snowden's leaks, WikiLeaks and similar revelations of government spying have led to legal challenges to government surveillance activity, some successful and others unsuccessful. In New Zealand, revelations about New Zealand's involvement in XKEYSCORE, allegedly an NSA-led mass data collection capability, happened close to revelations about GCSB involvement in the FBI's pursuit of Kim DotCom.[426] Those revelations led to changes to the GCSB's enabling legislation and a revamp of security and intelligence oversight in New Zealand.[427]

In the United States, Klayman obtained a preliminary injunction against the government's bulk data collection, but that judgment was later overturned.[428] However, 6 months earlier, the Court of Appeals for the Second Circuit had decided in *American Civil Liberties Union v Clapper* that the NSA's collection of bulk metadata of telephone call records violated s 215 of the PATRIOT Act.[429] The United States Congress subsequently passed the USA Freedom Act, which amended s 215 to explicitly prohibit the bulk collection of Americans' call records.[430] The Investigatory Powers Tribunal in

[422] Clive Walker "Investigative Journalism and Counter Terrorism Laws" (2017) 31 (1) *Notre Dame Journal of Law, Ethics and Public Policy* 129, at 135. In New Zealand this attitude is somewhat evident in *ad hominem* attacks on Nicky Hager, such as in Editorial "John Key hits back at Nicky Hager over GCSB claims" (23 March 2015) Newshub <www.newshub.co.nz>.

[423] Greenwald, above n 143, at 182–185.

[424] *Intelligence Activities and the Rights of Americans: Book II - Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities* 94th Congress 2nd Session, S Rept 90-755 (1976), at 3. A denial of Snowden's allegation of mass surveillance by the United States and the United Kingdom governments is documented in Robin Simcox *Surveillance after Snowden: Effective Espionage in an Age of Transparency* (The Henry Jackson Society, London, 2015), at 71–72.

[425] Julian Assange "What is WikiLeaks" (2006) Wikilieaks <wikileaks.org>.

[426] *Dotcom v Attorney-General* [2014] NZSC 199 and Patman and Southgate, above n 176, at 881.

[427] Patman and Southgate, above n 176, at 882 and 883.

[428] *Klayman v Obama* 957 F Supp 2d 1 (DC Cir 2015).

[429] *American Civil Liberties Union v Clapper* 785 F 3d 787 (2d Cir 2015).

[430] USA Freedom Act 50 USC § 1862 (United States).

the United Kingdom also found that the intelligence services had acted unlawfully in their collection and use of this type of Big Data intelligence provided by the NSA.[431]

Big Data intelligence could be shared through a single window system using the proposed legal framework. Public confidence in the government use of a single window to share intelligence is therefore likely to be affected by the general level of public distrust of government intelligence activities. Leigh argues that transparency of intelligence oversight and "vigilance in protecting human rights" will reduce media scrutiny and investigations of human rights abuses which undermine public confidence.[432] The approach recommended here will allay some of that distrust by publicly disclosing the way in which personal information will be treated. However, some public distrust is likely to remain because of the ongoing secrecy of the methods and content of the government's Big Data intelligence collection.

A tension exists between the government's need to establish and maintain public confidence and the government's need to maintain the trust of its intelligence partners. The publicity surrounding events such as the Snowden leaks reinforces the need for transparency in the protection of privacy and other human rights in the proposed legal framework. It seems that complete public confidence in government intelligence-sharing is an impossibility because of the secret nature of the intelligence material. The approach in the proposed legal framework aims to restore some public confidence in intelligence processes, specifically the processes for intelligence-sharing by customs administrations, without degrading the trust of intelligence partners. It does this by showing how personal information will be handled by customs administrations in accordance with the widely accepted principles of privacy law. To that end, Parts IV and V below describe the principles of privacy that have evolved in tort law and legislation..

## *IV The Tort of Privacy*

This Part is neither a comprehensive analysis of tort law, nor a comprehensive assessment of the torts that might arise through the use of the proposed legal framework. It provides an overview of the tort law that has evolved in relation to the use of personal information by government agencies.

The torts of intrusion and confidence are identified as the torts most relevant to sharing customs intelligence through a single window system. The state's protection of the individual from these torts when it is sharing personal information under the terms of the

[431] *Liberty v the Security Service, SIS and GCHQ* [2015] IPT/13/77/H.

[432] Ian Leigh "Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11" (2012) 27(5) Intelligence and National Security 722, at 724.

proposed legal framework is a condition of the public confidence and the mandate granted by the public, because: [433]

> A key idea… is that [civil society] building would affect the so-called "social contract" between the state and its citizens. The notion of a social contract captures the idea that state authority is based on the consent of its citizens, which forfeit some of their freedoms in exchange for the benefits of social order through the rule of law.

States are "instruments at the service of their people and not vice versa".[434] Christodoulidis and Tierney describe this as maintaining the essential link between the state and nation:[435]

> … public law has served the function of sustaining the link between state and nation – those key constructs of modernity – by giving the former authority – legitimate authority – in the management of the latter.

Many states have enacted laws to protect the individual's right to privacy, but there is no equivalent legislation to protect an individual's secrecy.[436] Instead, the privacy torts of breach of confidence or intrusion provide this protection in some circumstances. Accordingly, the state has a duty under evolving tort law to protect the privacy of individuals.

The specific legal protection for privacy is a recent development.[437] Privacy only appears in relatively advanced cultures. The eighteenth-century case of *Entick v Carrington*, discussed in Chapter Three, related to a physical intrusion into the home.[438] In Victorian Great Britain, the notion of privacy was still primarily one of physical seclusion and protection from intrusions or direct violations of physical privacy.[439]

---

[433] Verkoren and van Leeuwen, above n **Error! Bookmark not defined.**, at 466.

[434] Kofi Anan "Two Concepts of Sovereignty" *The Economist* (online edition, London, 18 September 1999) at 49.

[435] Emelios Christodoulidis and StephenTierney (eds) *Public Law and Politics: The Scope and Limits of Constitutionalism* (Ashgate, Aldershot, 2008), at 6.

[436] For example, the Official Information Act 1982 (New Zealand); Official Secrets Act 1889 (United Kingdom); Official Secrets Act 1972 (Malaysia); Espionage Act 18 USC § 792 (United States); Crimes Act 1961 (New Zealand), s 230; and Economic Espionage Act 18 USC § 1831-1839 (United States).

[437] Patrick O'Callaghan *Refining Privacy in Tort Law* (Springer Science & Business Media, Newcastle UK, 2012) and Natasha Stott Despoja "A Brief Look at the History of Privacy" (2007) 79(3) Australian Quarterly 60, at 60.

[438] *Entick v Carrington*, above n 266.

[439] David Vincent *I Hope I Don't Intrude: Privacy and its Dilemmas in Nineteenth-Century Britain* (Oxford University Press, Oxford, 2015), at 159–160.

In *Prince Albert v Strange*, the Court found that Prince Albert's confidence had been breached by the publication of his etchings. The Court found that this was an intrusion into his privacy:[440]

> … because it is an intrusion – an unbecoming and unseemly intrusion – an intrusion not alone in breach of conventional rules, but offensive to that inbred sense of propriety … if intrusion, indeed, fitly describes a sordid spying into the privacy of domestic life ….

*Wilkinson v Downton* introduced a new tort of physical harm through causing emotional distress for English Common Law in 1897, although privacy had not received explicit recognition as a tort in United Kingdom law at that time.[441] While the tort of defamation offered some protection to individuals, it in no way protected people's privacy generally.[442] A defence against the tort of defamation exists where facts, however embarrassing to the individual, may be aired in public, providing they are true.[443]

By 1996 there had been numerous attempts in the United Kingdom to legislate for improvements in the treatment of privacy by the press.[444] In United Kingdom law, a privacy tort also developed in respect of surveillance which "focussed instead on trespass to property and the interception of communications".[445]

In *Wainwright v Home Office,* the claimants sought relief for battery, humiliation and what they believed was an invasion of privacy, following a search by prison officers at Amesbury Prison, Leeds.[446] The search was not protected by statutory powers conferred on the prison officers.[447] The Wainwrights were subjected to battery, for which they

---

[440] *Prince Albert v Strange* [1849] EWHC Ch J20, (1849) 18 LJ Ch 120, (1849) 1 Mac & G 25, 41 ER 1171, at [698].

[441] *Wilkinson v Downton* [1897] 2 QB 57, [1897] EWHC 1 (QB).

[442] Peter Kaye *An Explanatory Guide to the English Law of Torts* (Barry Rose Law Publishers, Chichester, 1996), at 590.

[443] Todd et al, above n 316, at 862. Note that this premise was unsuccessfully challenged in the case of *Rhodes v OPO* [2015] UKSC 32, in which the mother of OPO sought an injunction against a father's (Rhodes) autobiography on the basis that it contained material that had the potential to emotionally harm the child, regardless of the truthfulness of that material. The Court discharged the injunction because it infringed too greatly on Rhodes' right to freedom of expression.

[444] Todd et al, above n 316, at 591.

[445] McKay, above n 152, at 152 para 5.09. See also *Khan v United Kingdom* [2000] ECHR 194, (2000) 31 EHRR 1016, [2000] ECHR 195, (2001) 31 EHRR 45 and *Malone v United Kingdom* (1984) 7 EHRR 14 (ECHR).

[446] *Wainwright v Home Office* [2003] UKHL 53, [2004] UKHRR 154, [2004] 2 AC 406, [2003] 4 All ER 969, 15 BHRC 387, [2003] 3 WLR 1137.

[447] At [7].

received damages, but they were unsuccessful in their claim of invasion of privacy.[448] In this regard, Lord Hoffmann stated:[449]

> What the courts have so far refused to do is to formulate a general principle of "invasion of privacy" (I use the quotation marks to signify doubt about what in such a context the expression would mean) from which the conditions of liability in the particular case can be deduced.

Lord Scott declared:[450]

> … whatever remedies may have been developed for misuse of confidential information, for certain types of trespass, for certain types of nuisance and for various other situations in which claimants may find themselves aggrieved by an invasion of what they conceive to be their privacy, the common law has not developed an overall remedy for the invasion of privacy. The issue of importance in the present case is whether the infliction of humiliation and distress by conduct calculated to humiliate and cause distress, is without more, tortious at common law.

The leading case for a tort of invasion of privacy in New Zealand is *Hosking v Runting*, which involved the publication of photographs of Hosking's children.[451] Although Hosking's claim was unsuccessful, the Court of Appeal suggested that a cause of action could exist where an individual has a reasonable expectation of privacy and the publicity in question would be considered highly offensive to an objective person.[452] *C v Holland* introduced a new privacy tort in New Zealand.[453] In *C v Holland*, the defendant covertly made and stored intimate video recordings of the plaintiff, which the plaintiff later discovered. Because Holland had not shown the recordings to anyone, the test that "publicity given to the facts would be considered highly offensive" could not be satisfied.[454] In this case, Whata J referred to the New Zealand Law Commission's recommendation that the tort of invasion of privacy should be left to the court.[455] *C v*

[448] At [12], [53], [54], [55] and [64].

[449] At [19].

[450] At [62].

[451] *Hosking v Runting* [2004] NZCA 34, [2005] 1 NZLR 1, which is another case involving the child of a celebrity.

[452] At [42].

[453] *C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672.

[454] *Hosking v Runting*, above n 451, at [15], [43] and [266].

[455] *C v Holland*, above n 453, at [83] and "Invasion of Privacy - Penalties and Remedies: Review of the Law of Privacy Stage 3 (NZLC R113)" (2010) New Zealand Law Commission <www.lawcom.govt.nz> at [R29].

*Holland* introduced a test for a tort of intrusion upon seclusion in which a plaintiff must show:[456]

> (a) an intentional and unauthorised intrusion;
> (b) into seclusion (namely intimate personal activity, space or affairs);
> (c) involving infringement of a reasonable expectation of privacy; and
> (d) that is highly offensive to a reasonable person.

Hunt argues that *C v Holland* replaces the publication test with one of intrusion into seclusion, meaning the plaintiff was secluded from public view when the intrusion occurred.[457] Hunt also notes that Whata J aimed to maintain consistency with the North American tort of intrusion.[458]

The Common Law in the United Kingdom, drawing on the rights set out in the European Convention for Human Rights (ECHR), developed further in *Campbell v Mirror Group Newspapers Limited.*[459] In the High Court, Morland J had established a clear test by stating:[460]

> In my judgment to succeed in her claim for breach of confidentiality Miss Naomi Campbell must establish three things.
>
> First that the details given by the publications complained of about her attendance at Narcotics Anonymous meetings have the necessary quality of confidence about them.
>
> Secondly that those details must have been imparted in circumstances importing an obligation of confidence.
>
> Thirdly that the publication of the details must be to her detriment.

In the House of Lords, Lord Hoffmann brought the ECHR into focus, stating:[461]

> In recent years, however, there have been two developments of the law of confidence, typical of the capacity of the common law to adapt itself to the

[456] *C v Holland*, above n 453, at [94].

[457] Chris DI Hunt "New Zealand's New Privacy Tort in Comparative Perspective" (2013) 13(1) OUCLJ 157, at 159.

[458] Ibid, and *C v Holland*, above n 453, at [94].

[459] *Campbell v Mirror Group Newspapers Limited* [2004] UKHL 22, [2004] 2 AC 457, [2 WLR 1232, [2004] 2 All ER 995 (HL). Campbell made a successful claim against Mirror Group Newspapers that was subsequently overturned in the Court of Appeal. Campbell appealed to the House of Lords, which confirmed the Court of Appeal's decision.

[460] At [37].

[461] At [46].

> needs of contemporary life. One has been an acknowledgement of the artificiality of distinguishing between confidential information obtained through the violation of a confidential relationship and similar information obtained in some other way. The second has been the acceptance, under the influence of human rights instruments such as article 8 of the European Convention, of the privacy of personal information as something worthy of protection in its own right.

In regard to the photographs that were published, Lord Nicholls noted:[462]

> In general photographs of people contain more information than textual description. That is why they are more vivid. That is why they are worth a thousand words. But the pictorial information in the photographs … added nothing of an essentially private nature. They showed nothing untoward …. The group photograph showed Miss Campbell in the street exchanging warm greetings with others on the doorstep of a building. There was nothing undignified or distrait about her appearance. The same is true of the smaller picture on the front page.

The Court found that it must balance the right of freedom of expression, associated with the publication of photographs and an accompanying article, with Campbell's ECHR right to privacy.[463] In this regard, Lord Hope noted:[464]

> The jurisprudence of the European Court of Human Rights explains how these principles are to be understood and applied in the context of the facts of each case. Any restriction of the right to freedom of expression must be subjected to very close scrutiny. But so too must any restriction of the right to respect for private life. Neither article 8 nor article 10 has any pre-eminence over the other in the conduct of this exercise … since they are of equal value in a democratic society.

This contrasts with the European case of *Von Hannover v Germany*. In that case, the Court found that the publication of photographs of activities in the daily life of Princess Caroline and her children was a breach of art 8 of the ECHR.[465]

*Murray v Express Newspapers Plc* elaborated on the application of privacy and freedom of expression. *Murray* was another case involving photographs of a celebrity's children. In this case, an appeal was made on behalf of JK Rowling's infant son, David Murray,

[462] At [31].

[463] ECHR, above n 231, arts 8 and 10.

[464] *Campbell v Mirror Group Newspapers Limited*, above n 459, at [113].

[465] *Von Hannover v Germany* [2004] ECHR 294.

against the publication of photographs of the child. [466] It was claimed that the publication was an infringement of "his right to respect for his private life, contrary to art 8 of the European Convention on Human Rights".[467] The United Kingdom Court of Appeal allowed the appeal, stating "the facts of *Hosking v Runting,* as in this case, are not the same as in Campbell".[468] The Court also declared:[469]

> It seems to us … the law should indeed protect children from intrusive media attention, at any rate to the extent of holding that a child has a reasonable expectation that he or she will not be targeted in order to obtain photographs in a public place for publication which the person who took or procured the taking of the photographs knew would be objected to on behalf of the child …. David had a reasonable expectation of privacy and it seems to us to be more likely than not that, on the assumed facts, it would hold that the Art.8/ 10 balance would come down in favour of David.

The cases of *Hosking v Runting*, *Campbell v Mirror Group Newspapers* and *Murray v Express Newspapers* signal that, while there is no liability for the publication of unwanted photographs made in public, a tort exists in respect of intrusion, confidence and the publicity of private facts.[470] Penk notes that *Hosking* is unlike United States cases.[471] This is because of differences in the constitutional frameworks and differing social climates.[472]

These cases involved private individuals and companies as plaintiffs and respondents. However, the tort also creates a potential liability for a customs administration that discloses personal information through information-sharing for border protection.[473] For example, an individual might suffer reputational harm if a customs administration disclosed that the individual was suspected of committing a crime, or that the individual associated with criminal suspects. A customs administration could also be liable under

---

[466] *Murray v Express Newspapers Plc* [2008] EWCA Civ 446, [2009] Ch 481,[2008] 3 WLR 1360, [2008] ECDR 12, [2008] EMLR 12 [2008] 2 FLR 599, [2008] 3 FCR 661, [2008] HRLR 33, [2008] UKHRR 736, [2008] Fam Law 732 (CA).

[467] At H2.

[468] At [51].

[469] At [57].

[470] Todd et al, above n 316, at 971.

[471] Stephen Penk "Common Law Privacy Protection in other Jurisdictions" in Stephen Penk, Rosemary Tobin, Khylee Quince, Bill Hodge, Donna Maree Cross, Warren J Brookbanks, Natalya King, Pauline Tapp, Hon Judge David Harvey *Privacy Law in New Zealand* (2nd ed, Brookers, Wellington, 2016) 113, at 131–132.

[472] Ibid, and *Hosking v Runting*, above n 451, at [76].

[473] See *Brown v Attorney-General* [2006] DCR 630, in which the Court found that the Police had breached Brown's right to privacy by publishing a flier containing Brown's photograph and address.

the tort of negligence, despite having legislated powers to disclose that information.[474] Cooke P suggested in *Baigent's Case* that remedies should exist for breaches of legislated rights by the state.[475] In such cases the issue of proportionality, or the balance of human rights with public policy, arises.[476] The issue requires decisions in respect of whether "… a legitimate public policy is either too broad or has imposed a disproportionate burden on certain individuals".[477] In the Irish case of *Kennedy v Ireland*, substantial damages were awarded because the state infringed the plaintiff's right to privacy.[478] On this matter, Elias CJ stated in an address at the University of Hong Kong:[479]

> The better view seems to me that whether public bodies are liable for the negligent exercise of statutory powers does not turn on whether their use is lawful.

She quoted Gaudron J as follows:[480]

> Rather, it is a duty called into existence by the common law by reason that the relationship between the statutory body and some member or members of the public is such as to give rise to a duty to take some positive step or steps to avoid a foreseeable risk of harm to the person or persons concerned.

States have enacted various laws to implement the right to privacy while the tort of privacy has been evolving. The next Part examines international developments in privacy legislation from which the commonly accepted privacy principles are identified for present purposes. The inclusion of these principles in the proposed legal framework should provide some protection to the public against harm from intrusion and breaches of confidence.

---

[474] For a discussion of the tensions between negligence in tort law and the state's use of legislated powers, see Jenny Steele *Tort Law: Text, Cases and Materials* (2nd ed, Oxford University Press, Oxford, 2010), at 404. Note that Harlow argues that state agencies are unlikely to be guided by tort law in Carol Harlow *State Liability: Tort Law and Beyond* (Oxford University Press, Oxford, 2004), at 127.

[475] *Simpson v Attorney-General* [Baigent's Case] [1994] 3 NZLR 667 (CA). In this case the right to freedom from unreasonable search and seizure was breached.

[476] McKay, above n 152, at 50 para 2.122.

[477] Ibid, para [2.124]. See also *Sporrong and Lonroth v Sweden* (1983) 5 EHRR 35, at [69] and [73].

[478] *Kennedy v Ireland* [1987] IR 587.

[479] Sian Elias CJ "Public Actors and Private Obligations – a Judicial Perspective" (the University of Hong Kong Obligations VII Conference, University of Hong Kong Faculty of Law, 18 July 2014), at 6.

[480] *Crimmins v Stevedoring Industry Finance Committee* [1999] HCA 59; 200 CLR 1; 74 ALJR 1; 167 ALR 1, at [25].

## *V Privacy Legislation*

This Part summarises the recent global development of privacy legislation and identifies the privacy principles that are included in the proposed legal framework.

A number of countries have chosen to implement the right to privacy through data protection legislation. In January 2015, a survey found that privacy legislation existed in 109 states and legislation was under development in a further 22 states.[481] There are differences in the data protection laws of these states[482]. Differences in data protection laws represent the variety of state responses to the need for privacy, which in turn may reflect different cultural and religious approaches to privacy protection.[483] Nonetheless, while privacy laws vary from state to state, some privacy principles, whilst not universally adopted, are common amongst those states that have enacted privacy law.[484]

Most notably, the Privacy Principles enshrined in the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data 1980, subsequently updated as the OECD Privacy Framework, have been implemented in the Privacy Act 1993 of New Zealand.[485] The principles are listed in the OECD Privacy Framework under the headings "Basic Principles of National Application" and "Basic Principles of International Application: free flow and legitimate restrictions". These principles were adopted by the 36 member-states of the OECD and the EU. The principles are echoed in the legislation of Australia, Canada, Japan, and Argentina. The principles of the OECD Privacy Framework are referred to as the "Privacy Principles" in the remainder of this work. They are presented here as the most widely accepted expression of public expectations for privacy treatment.

---

[481] Graham Greenleaf "Global Tables of Data Privacy Laws and Bills (4th ed, January 2015)" (2015) Australasian Legal Information Institute <www2.austlii.edu.au> and Graham Greenleaf "Global Data Privacy Laws 2015: 109 Countries with European Laws now in a Minority" (2015) 133 Privacy Laws & Business International Report 14.

[482] For example, see the overview of privacy laws in the "ICT Regulation Toolkit" (2009) ITU <ictregulationtoolkit.org>.

[483] Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?", above n 331, at 69.

[484] It is interesting to note that the development of the United Nations, privacy and other fundamental human rights has meant that where the UN bodies have jurisdiction over these rights, state sovereignty is "no longer as relevant as before", according to Lawrence M Friedman in *The Human Rights Culture: A Study in History and Context* (Quid Pro Books, New Orleans, 2011), at 143.

[485] OECD "Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data" (1980) OECD <www.oecd.org> and OECD Privacy Framework, above n 12. See also New Zealand Law Commission, above n 390, at 83 and Privacy Act 1993 (New Zealand).

As such, they are accepted as the principles that are most suitable for inclusion, wherever possible, in the proposed legal framework. The Privacy Principles are as follows.[486]

### *A Privacy Principles: Basic Principles of National Application*

#### *1 Collection Limitation*

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

#### *2 Data Quality*

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

#### *3 Purpose Specification*

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

#### *4 Use Limitation*

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification principle except:

(i) with the consent of the data subject; or

(ii) by the authority of law.

#### *5 Security Safeguards*

Personal data should be protected by reasonable Security Safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

#### *6 Openness*

There should be a general policy of Openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

#### *7 Individual Participation*

Individuals should have the right:

[486] OECD Privacy Framework, above n 12, at 14–16.

(i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

(ii) to have communicated to them, data relating to them –

a. within a reasonable time;

b. at a charge, if any, that is not excessive;

c. in a reasonable manner; and

d. in a form that is readily intelligible to them;

(iii) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(iv) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended

*8 Accountability*

A data controller should be accountable for complying with measures which give effect to the principles stated above.

*B Privacy Principles: Basic Principles of International Application*

*1 A data controller is accountable*

A data controller remains accountable for personal data under its control without regard to the location of the data. This principle extends the responsibility of the data controller in the Accountability principle of the Basic Principles of National Application.

*2 Limit restrictions to transborder flows of personal data*

A member country should refrain from restricting transborder flows of personal data between itself and another country where:

(i) the other country substantially observes these Guidelines; or

(ii) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

*3 Restrictions are proportionate to risk*

Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

### *C Domestic Implementation of the Privacy Principles*

The principles of the OECD Privacy Framework have been developed through collaboration by the 32 OECD member states with the participation of the 27 member states of the EU.[487]

The privacy laws of a selection of states are measured against these principles from the OECD Privacy Framework in Table 3. The states examined are New Zealand, Australia, the EU, Japan, Canada, Argentina and the Russian Federation.[488] These states were chosen as examples of the privacy law that has evolved in the different regions and cultures of North America, South America, Asia, Europe and Oceania.

**Table 3. Application of OECD principles in a selection of states**

Notes:

† A Privacy Commissioner has a statutory role to fulfil 'data controller' duties in respect of advocacy for individuals and deciding on complaints about breaches of the principles.

* Government guidelines recommend that companies designate a manager called a Chief Privacy Officer (CPO).[489]

Δ The legislation does not explicitly require agencies to give reasons if a request to acknowledge or provide access to information is denied.

| | New Zealand | Australia | European Union | Japan | Canada | Argentina | Russian Federation |
|---|---|---|---|---|---|---|---|
| **Basic principles of national application** | ✓ Stipulated in the legislation | | | × No explicit stipulation | | | |
| Collection Limitation principle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| Data Quality principle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Purpose Specification principle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| Use Limitation principle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| Security Safeguards principle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Openness principle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| Individual Participation principle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Accountability principle | ✓† | ✓† | ✓ | ✓* | ✓† | ✓Δ | × |
| **Basic principles of international application** | | | | | | | |
| A Data Controller is Accountable | ×† | ✓† | ✓ | P* | ✓† | ✓Δ | × |
| Limit restrictions to transborder flows of personal data | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| Restrictions are proportionate to risk | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × |

[487] OECD Privacy Framework, above n 12, at 2–3.

[488] Privacy Act 1993 (New Zealand); Privacy Act 1988 (Australia); Directive 95/46/E, above n 300; Amended Act on the Protection of Personal Information 2015 (Japan); Privacy Act 1983 (Canada); Personal Information Protection and Electronic Documents Act 2000 (Canada); Data Protection Act 2000 (Argentina) and Law of the Russian Federation on Information, Informatization, and Information Protection 1995 (Russian Federation).

[489] Ministry of Economy, Trade and Industry "Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information" (12 November 2017) Ministry of Economy, Trade and Industry <www.meti.go.jp>, at 33.

The Global Liberty Internet Campaign (GLIC) notes that Russia, which has data protection laws that do not comply with the OECD Privacy Framework, has not established a central regulatory body for data protection.[490] GLIC suggests that the effectiveness of Russia's laws is unclear.[491] Russia is a member of the Council of Europe, but it has not signed or ratified two of the Council's principal Conventions that are aimed at protecting human rights and personal information.[492]

Even so, while the principles of the OECD Privacy Framework exist in one form or another in some states, other laws can over-ride the protection they are intended to provide. The OECD Privacy Framework allows this through an exception to the Use Limitation principle.[493] These provisions are generally intended to improve the security and effectiveness of law enforcement activities. For example, the EU Data Protection Directive includes:[494]

> This Directive shall not apply to the processing of personal data… to processing operations concerning public security, defence, State security (including economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

The Privacy Act 1993 (New Zealand) contains similar exclusions that over-ride a government agency's responsibility to inform an individual of the information held about that individual. It states:[495]

> It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds… that non-compliance is necessary-
>
> (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
>
> (ii) for the enforcement of a law imposing a pecuniary penalty; or

---

[490] "Privacy and Human Rights: An International Survey of Privacy Laws and Practice" (2010) GLIC <glic.org>.

[491] Ibid.

[492] European Convention for the Protection of Human Rights and Fundamental Freedoms ETS 5 (1950) and Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ETS 108 (1981).

[493] OECD Privacy Framework, above n 12, at 14, s 10(b).

[494] Directive 95/46/EC, above n 300, art 3 (2).

[495] Section 6, principle 3(4).

(iii) for the protection of the public revenue; …

These exclusions do not preclude the covert collection and use of personal information for law enforcement purposes, including the protection of tax revenue. The provisions have the effect of keeping the individual ignorant of the state's information holding, thereby nullifying the individual's right and ability to view that information and correct any errors (the Individual Participation principle**)**. Furthermore, the Privacy Act 1993 (New Zealand) stipulates that if other statutes have provisions contrary to its privacy principles, the provisions of those other statutes prevail.[496] The New Zealand Law Commission is responsible for undertaking a continuous review of New Zealand law in order to recommend and promote law reform and development.[497] It reviewed the law enforcement exclusions and made recommendations in regards to the law enforcement and criminal disclosure grounds for refusing access requests and for disclosing and sharing personal information.[498]

The New Zealand Government reported that it had begun work on initiatives to implement 12 of the recommendations, following its receipt of the Law Commission's report.[499] It agreed to work on a further 39 of the recommendations and identified 55 recommendations that it believed required further investigation and 19 recommendations that it would defer or not pursue.[500] Provisions were introduced to the Privacy Act 1993 that require government approval through an Order in Council for any exemptions or modifications to the privacy principles for new information-sharing agreements between New Zealand government agencies.[501] The agreements must be prepared in consultation with the Privacy Commissioner and any person or organisation that the agencies consider represents the interests of the classes of individuals whose personal information will be shared under the agreement.

The Law Commission's recommendations and review did not however consider the effect of the law enforcement exclusions on the implementation of other privacy principles, such as the Data Quality principle, which are unrelated to the disclosure of information.

---

[496] Section 7.

[497] "Briefing Paper for the Minister Responsible for the New Zealand Law Commission" (2011) New Zealand Law Commission <www.lawcom.govt.nz>, at 4.

[498] "Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4 (R123)" (2011) New Zealand Law Commission <www.lawcom.govt.nz>, at 232–248.

[499] "Government Response to Law Commission Report on the Review of the Privacy Act 1993" New Zealand Law Commission (2011) <www.lawcom.govt.nz>, at 4-6.

[500] Ibid.

[501] Sections 96A–96Z.

The Australian privacy principles have similar exclusions for law enforcement. For example, principle 6 provides that individuals can be denied access to information held about them, if providing access would be likely to prejudice:[502]

> (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
> (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
> (iii) the protection of the public revenue.

There are also provisions in other New Zealand Acts and legislative instruments that over-ride the privacy legislation and which are relevant to intelligence-sharing in support of a single window. For example, an Order in Council enables the Department of Internal Affairs to share the passport information of student loan borrowers and child custody payment defaulters with the Inland Revenue Department.[503] Another example is the Customs and Excise Act 1996 which empowers the Chief Executive of the New Zealand Customs Service to disclose information to an overseas agency, body, or person, whose functions include:[504]

> (a) the prevention, detection, investigation, prosecution, or punishment of offences that are, or that if committed in New Zealand would be, –
> (i) customs offences of any kind; or
> (ii) other offences punishable by imprisonment; or
> (b) the processing of international passengers at the border by public authorities; or
> (c) border security; or
> (d) the enforcement of a law imposing a pecuniary penalty; or
> (e) the protection of public revenue.

Toy argues that the existing privacy legislation in New Zealand is insufficient to meet the needs of international data exchanges.[505] Specifically, Toy argues that the Privacy Act 1993 does not give remedies to a data subject "against a third party who has received their personal information, once it has been transferred out of New Zealand".[506]

---

[502] Privacy Act 1988 (Australia), at Part III, Division 2, s14. See also Office of the Australian Information Commissioner "Privacy Fact Sheet 2: National Privacy Principles" (July 2011) OAIC <www.oaic.gov.au>.

[503] Privacy (Information Sharing Agreement Between Inland Revenue and Internal Affairs) Order 2014 LI 2014/223 (New Zealand).

[504] Section 281.

[505] Alan Toy "Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity" (2010) 24(2) NZULR 223, at 223.

[506] At 224.

In light of the weakness identified by Toy and the exempting provisions discussed above, care must be taken to ensure compliance with the spirit and intent of the OECD Privacy Framework and domestic privacy legislation. This compliance is necessary to ensure on-going compatibility with the other jurisdictions with which a customs administration may wish to share intelligence.

Recognising the need to ensure the compatibility of privacy protections between states, the proposed legal framework adopts the Privacy Principles of the OECD Privacy Framework as the minimum standard for privacy protection. The proposed legal framework rejects the notion that law enforcement and security activities should be universally exempted from privacy protection. The discussion above illustrates that many privacy principles, such as the Data Quality and Security Safeguards principles, do not conflict with the need to keep information secret from data subject. The privacy principles can be adapted to account for the need to maintain secrecy for some information. This is discussed in the next Part.

## *VI Privacy Principles Applied to the Legal Framework*

This Part identifies the Privacy Principles that can be adapted for use as checks and balances on customs intelligence-sharing activity in the proposed legal framework. Even Machiavelli recognised the need for checks and balances to constrain the use of sovereign power, saying:[507]

> … it is to be noted how easily men are corrupted, even when they are good and well trained …. Lawmakers should bear this in mind when they make laws to restrain evildoing and to remove the possibility of evildoing with impunity.

These checks and balances will contribute to improved public confidence. Although the OECD Privacy Framework's principles are not universal, it is important to include them in customs intelligence-sharing processes. As well as being the most widely accepted principles, the 32 states that have adopted the OECD Privacy Framework require the personal information to be afforded equivalent protection when transmitted and stored offshore. This is made explicit in the Basic Principles of International Application and is important to maintain public confidence in each state's information-sharing and law enforcement activities. The New Zealand Law Commission made the following remarks on the potential effect on public confidence in data processing:[508]

> Technology can facilitate vast collections and disclosures of personal information that may affect a large number of people, even though the effects on individuals may be small. Online data collection and use can

[507] Machiavelli, above n 161, at 260.

[508] New Zealand Law Commission, above n 390, at 350.

> affect an individual's ability to control his or her personal information without necessarily resulting in demonstrable "harm". While there may sometimes be little measurable harm caused in individual terms, the impact in terms of the societal value of privacy and public confidence may be significant.

In the United States, social media technology companies such as Google, Facebook and Twitter are under investigation in regard to the extent to which they may have been used to influence the 2016 United States elections.[509] This investigation, and the media attention associated with it, highlights the public concern regarding the extent to which these companies collect and use personal information.[510]

In the absence of an individual's right to know and access the information held about them, the Privacy Principles of the OECD Privacy Framework can be applied as follows.[511]

### *A Collection Limitation*

This principle cannot be strictly applied in customs intelligence processes. Customs administrations must have some powers to obtain information without the knowledge and consent of the data subject.[512] The sources of that information may have collected the information for other purposes, for example in the facilitation of air travel. Permitting collection only for specific purposes will limit the accumulation of personal information, even in the absence of the data subject's knowledge or consent. This Privacy Principle is not addressed in the legal framework because the collection phase of the intelligence lifecycle is outside the scope of activities it covers. However, this principle is partially addressed in the sharing phase of the lifecycle through controls that limit the purposes for which information can be shared.

### *B Data Quality*

Customs administrations will be obliged to keep information accurate and up to date, but individuals will not be able to notify customs administrations of inaccurate information in intelligence that is kept secret from them. Reliance on incorrect or inaccurate information can harm others as well as the intended data subject. Examples include many cases of innocent people being denied travel because they have been included in "no-fly"

---

[509] *Daily Edition: Daily Digest/Senate Committee Meetings* 115th Congress, 1st Session Issue: Vol 163, No 177 (1 November 2017), at D1154.

[510] Sabrina Siddiqui "'From Heroes to Villains': Tech Industry faces Bipartisan Backlash in Washington" *The Guardian* (online edition, Washington, 26 September 2017).

[511] "OECD Privacy Framework, above n 12, at 14, ss 7–12.

[512] For example, Customs and Excise Act 1996 (New Zealand), ss 21, 38G, 38H – 38K, 280A – 280M, 282J and 282L.

lists which remain inaccessible to the public.[513] It is also alleged that "no-fly" lists have been used to target individuals critical of the United States Government, the WTO and the World Bank.[514] Another example of inaccurate intelligence leading to a breach of human rights is the case of *El-Masri v Former Yugoslav Republic of Macedonia*.[515] El-Masri claimed he was kidnapped in Macedonia, tortured and transported to Afghanistan for detention because he had been mistakenly identified as a person with terrorist connections. A United States Senate investigation into CIA detentions later revealed that two detainees had been held because of "information fabricated by a CIA detainee subjected to the CIA's enhanced interrogation techniques".[516] The investigation reported that El-Masri and other detainees were wrongfully held.[517]

Correcting inaccurate information is important because "by virtue of being exchanged, repeated and circulated, the shared information acquires legitimacy by means of a self-preferentiality which stands for truth".[518]

### *C Purpose Specification*

In customs intelligence processes, information may be collected through intelligence processes without the knowledge or consent of the data subject, so the subject may be unaware of the fact that information has been collected or the purposes for which the information will be used. Information may also be supplied to customs by other sources and used for purposes other than which it was originally collected, for example in support of "the prevention, detection, investigation, prosecution, or punishment of offences", by invoking the exemption allowed for in the "Use Limitation principle".[519] However, information shared between customs administrations using the proposed legal framework

---

[513] Jeffrey Kahn *Mrs. Shipley's Ghost: The Right to Travel and Terrorist Watchlists* (University of Michigan Press, Ann Arbor, 2013), at 2 and 157 and Jeffrey L Thomas *Scapegoating Islam: Intolerance, Security, and the American Muslim* (ABC-CLIO, Santa Barbara, 2015), at 45 – 47, 152 and 166.

[514] C William Michaels *No Greater Threat: America After September 11 and the Rise of a National Security State* (Algora Publishing, New York, 2007), at 150 and 422.

[515] *El-Masri v Former Yugoslav Republic of Macedonia* [2012] ECHR 2067, (2013) 57 EHRR 25, 57 EHRR 25, 34 BHRC 313. See also Lee Ferran "Court: CIA Tortured German During Botched Rendition" (2012) ABC News <abcnews.go.com>.

[516] Senate Select Committee on Intelligence *Unclassified: Committee Study of the Central Intelligence Agency's Detention and Interrogation Program* (United States Senate, Washington DC, 13 December 2012), at 21 and 154 – 157. Note that El-Masri is identified in that document as "al-Masri".

[517] At 159.

[518] Karine Cote-Boucher "The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada's Smart Border" (2008) 5(2) Surveillance and Society 142, at 149.

[519] OECD Privacy Framework, above n 12, at 14, allows other uses of information without the data subject's knowledge "by the authority of [another] law".

will be limited to the information to specific purposes. The Purpose Specification principle also requires that data should be destroyed when it is no longer required.[520]

*D Use Limitation*

The Use Limitation principle is affected by the same conditions regarding the knowledge and consent of the data subject that apply to the Collection Limitation and Purpose Specification principles listed above.

The proposed legal framework enables information that is collected for other purposes to be shared and used by customs administrations for law enforcement purposes, under the authority of existing laws that enable the sharing and use of that information.

*E Security Safeguards*

An important implication of the Use Limitation principle, the Security Safeguards principle and the Data Quality principle is that intelligence should be held no longer than it is actually required. Storing intelligence for longer than required increases the risk that over time it becomes:

(i) used for unintended or unauthorised purposes;

(ii) inaccurate and is not updated; or

(iii) devalued and, subsequently, security controls are weakened and it is inappropriately disclosed.

These risks, also commonly associated with Big Data, are mitigated by controls in the legal framework that specify information is only obtained and used for specific purposes and then destroyed when that information is no longer required. Controls are also in place to ensure appropriate security for personal information.

*F Openness*

The proposed legal framework satisfies the Openness principle by making the practices and policies for handling personal data clear. Public access to the terms of the agreement will allow individuals to know how their information will be treated and what privacy assurances can and cannot be provided when their information is shared with other customs administrations.

*G Individual Participation*

The Individual Participation principle specifies that a data subject should be able to enquire about a customs administration's collection of their information and correct that information where it is inaccurate or out-of-date.

[520] OECD Privacy Framework, above n 12, at 57 and Privacy Act 1993 (New Zealand), s6, principle 9.

The Individual Participation principle cannot be satisfied in customs intelligence-sharing processes. This is because intelligence information often must remain secret to protect law enforcement methods and operations.[521] Instead, the proposed legal framework contains provisions for each state to appoint a data controller to advocate on the behalf of the rights of individuals.

### *H Accountability*

The Accountability principle is observed through the implementation of data controllers, which are a feature of the OECD Privacy Framework.[522] The New Zealand Privacy Commissioner recognised the need for accountability in intelligence processes in 1998, stating:[523]

> My view is that the role of intelligence organisations should be kept to a tight brief, accountability mechanisms should apply, and there should be redress for actions of intelligence organisations breaching individual rights, including the right to privacy.

In New Zealand, the Privacy Commissioner may receive and investigate complaints about privacy breaches by government agencies and public companies.[524] However, while it has moral weight, the Privacy Commissioner has no power to impose penalties or remedies for any breach that is discovered and can only use best endeavours to secure a settlement between the parties.[525] A complainant can, however, bring a complaint to the Human Rights Tribunal.[526] The Human Rights Tribunal has the power to award damages or other relief it thinks fit.[527]

A privacy complaint related to the administration of government may also be made to the Office of the Ombudsmen.[528] The Office of the Ombudsmen is required to consult with the Office of the Privacy Commissioner to determine how the complaint should be dealt with.[529] However, the Office of Ombudsmen only has the power to issue a report

[521] See also the definition of intelligence in the Glossary.

[522] OECD Privacy Framework, above n 12, at 16.

[523] Marie Shroff *Necessary and Desirable: Privacy Act 1993 Review Highlights* (Privacy Commissioner, Wellington, 1998).

[524] Privacy Act 1993.

[525] Section 74.

[526] Sections 82 and 83.

[527] Section 85.

[528] Ombudsmen Act 1975 (New Zealand), s13.

[529] Section 17A.

of its opinion.[530] Much like the Privacy Commissioner, it has no power to impose penalties or remedies for any privacy breach.

The legal framework puts accountability mechanisms in place by including a data controller to ensure intelligence collection, handling, use and sharing complies with the privacy rights of individuals. Unlike the Privacy Commissioner or the Ombudsmen and the Human Rights Tribunal, all of which are external to the customs administration, the data controller is an internal role. The data controller is accountable for the customs administration's treatment of personal information. The data controller is responsible for receiving and responding to enquiries from individuals about their personal information. The data controller is also responsible for conducting audits to ensure the specified information handling controls are consistently applied.

The data controller exists within the customs administration as a central point of contact that is accountable for the organisation's compliance with the terms of the legal framework. This role differs from that of an external or independent oversight body. It has direct access to customs information and processes, whereas an external or independent oversight body generally has access only to information submitted to it as part of an investigation or review. For example, the Inspector-General of Intelligence and Security, the Privacy Commissioner and the Office of the Ombudsmen in New Zealand have varying powers to conduct an inquiry, request information, review processes and investigate particular complaints. Nevertheless, they do not have powers to enter a government agency and audit all the intelligence it holds.[531]

Thus, the data controller is a transparent mechanism for states to advocate on an individual's behalf when individuals must remain unaware of the sharing and use of their personal information. This will ensure the underlying intent of the Privacy Principles is achieved. Advocacy on behalf of individuals should not impede the right of individuals to begin proceedings against a customs administration for a breach of privacy. This advocacy will help states to meet the goals of art 8 of the UDHR, recognising that intelligence functions operate in an environment of secrecy.[532]

### *I Absence of a Centralised Database*

The Data Quality, Use Limitation, Purpose Specification and Security Safeguards principles are strengthened by the fact that the proposed legal framework does not use a centralised database. In the approach proposed here, customs administrations supply

[530] Sections 22-24.

[531] Intelligence and Security Act 2017 (New Zealand), s 158; Privacy Act 1993 (New Zealand, ss 13 and 22; and Ombudsmen Act 1975 (New Zealand), ss 18 and 19.

[532] Article 8: Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.

intelligence to other states on a case-by-case basis. The purposes for which information will be used are clearly set out and there are controls on access to information

#### *J Basic Principles of International Application*

The proposed legal framework conforms to the OECD Privacy Framework basic principles of international application as follows.

##### *1 A data controller is accountable*

As discussed above, customs administrations are required to appoint a data controller.

##### *2 Limit restrictions to transborder flows of personal data*

The principle states that transborder flows of personal data should not be restricted between countries that substantially observes the privacy guidelines. The approach recommended here enables transborder flows of personal data with a mechanism that implements the privacy principles to the greatest possible extent.

##### *3 Restrictions are proportionate to risk*

The principle states that any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing. The privacy principles, including security safeguards, are implemented to the greatest possible extent to enable sensitive personal information to be shared with adequate protection, for appropriate purposes.

### *VII Privacy Principles, Solove's Taxonomy and the Intelligence Lifecycle*

This Part examines the privacy principles that are included in the legal framework in the context of Solove's taxonomy for privacy.[533] The analysis suggests that an individual's comfort with the treatment of privacy will be improved by including privacy principles in this manner. However, an individual is unlikely to be completely assured that customs intelligence processes will treat their privacy properly. This is because the processes under consideration only cover part of the intelligence lifecycle. The analysis does not address privacy concerns associated with intelligence collection by customs or other government agencies, nor does it address the way intelligence is used or handled prior to its receipt by a customs administration.

The extent to which the Privacy Principles apply to each phase of the intelligence lifecycle is illustrated in Figure 10.

[533] Solove, above n 319.

**Figure 10. The Privacy Principles and thesis scope mapped to Solove's taxonomy of privacy**

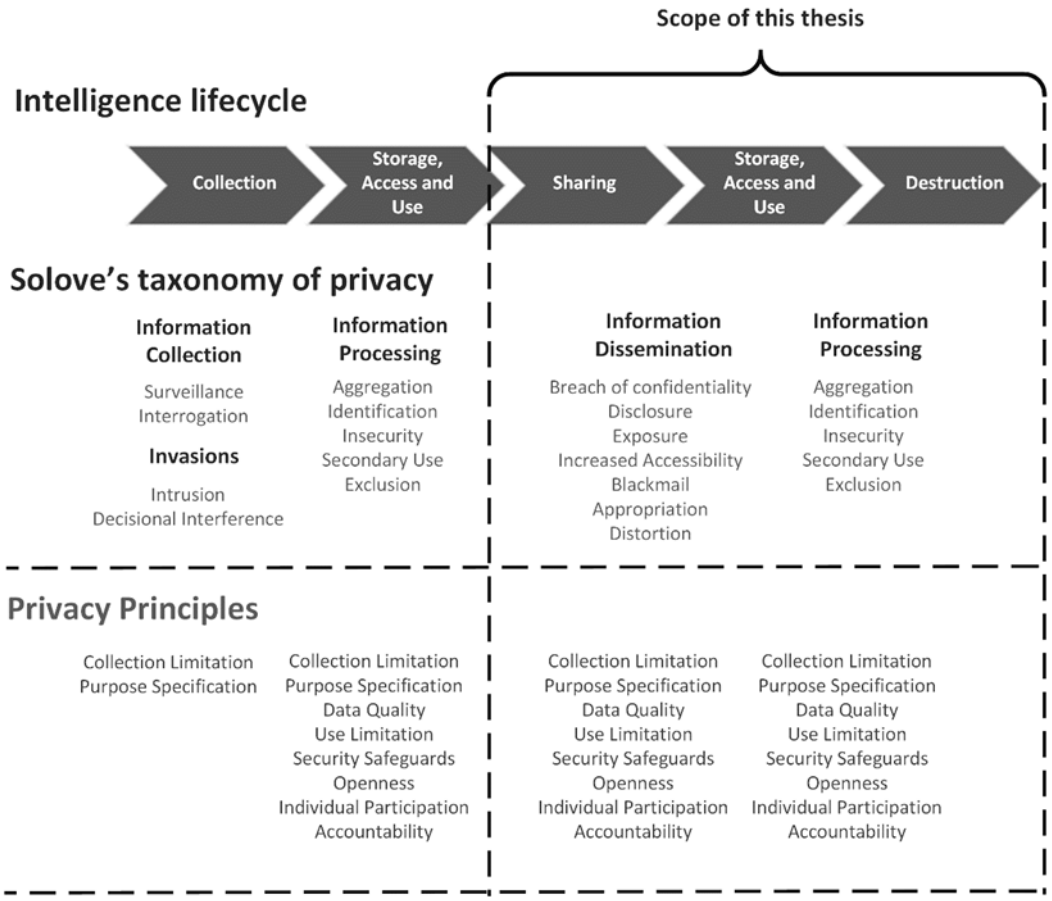



Figure 10 shows that the legal framework does not implement Privacy Principles in every phase of the intelligence lifecycle. Nor does it fully implement every Privacy Principle in the phases of the lifecycle that fall within its scope. However, Privacy Principles are implemented to the greatest possible extent within the limits imposed by the need for secrecy in security and law enforcement intelligence processing. The implementation of Privacy Principles in this way is a significant improvement as customs information-sharing agreements have typically omitted controls for the treatment of privacy.[534]

## *VIII Chapter Summary*

This Chapter has identified the privacy principles that should be expressly addressed to improve public confidence. The Privacy Framework of the OECD is the most widely accepted public expression of privacy values. The inclusion of these principles in the legal framework should improve public confidence in the intelligence-sharing done by customs administrations. This is needed because of changing public attitudes to government intelligence activities since the 9/11 terrorist attacks and the widespread publicity surrounding the Snowden leaks and Wikileaks.

[534] The treatment of privacy in other customs information-sharing arrangements is discussed in Chapter Five.

The extent to which the Privacy Principles can be implemented was mapped to the intelligence lifecycle and Solove's taxonomy of privacy. From that exercise, it is evident that the legal framework cannot address all the potential harms associated with the intelligence lifecycle. Nonetheless, public confidence in the treatment of personal information in customs intelligence-sharing processes can be improved by using a single window system and the legal framework proposed here. The improvement in public confidence in customs intelligence-sharing is not guaranteed. Public acceptance of the legal framework with the inclusion of these principles could be tested in forums such as parliamentary debate, select committee processes and the courts.

The extent to which terms in existing agreements and models meet the privacy and operational needs of an intelligence-sharing agreement for the single window system are discussed in the next Chapter.

# Chapter Five – How Other Arrangements Compare

This Chapter provides support for the claim made in the logic of the thesis that there is currently no law that enables customs administrations to share intelligence electronically and in real-time for risk management purposes. It brings together the ideas discussed in the previous Chapters and creates a set of measures to evaluate the suitability of a legal framework for sharing intelligence through a single window system. The set of measures will be used to compare the agreements that are discussed in this Chapter with the legal framework proposed in Chapter Six.

Thirty bilateral and multilateral agreements and six agreements for other models of information-sharing were evaluated. This evaluation included all the agreements that enable customs information-sharing that were accessible when the evaluation was undertaken. Some agreements were not publicly accessible and were supplied specifically for this thesis. This Chapter summarises the evaluation, discusses a selection of the agreements and highlights the main findings.

The dual purposes of the analysis in this Chapter are to demonstrate:

1. that existing agreements that enable customs administrations to share information would not enable intelligence-sharing through a single window system; and
2. the extent to which existing customs information-sharing agreements, and a small sample of other models for information-sharing, implement the elements essential to the success of the proposed legal framework.

Part I lists as measures the qualities needed for a legal framework to enable real-time intelligence-sharing via a single window system; to enable trust between states that intelligence will be handled appropriately and used only for approved purposes; and to enable public confidence through the protection of human rights and the careful control of personal information.

Part II discusses the bilateral agreements established for customs administrations to share information, with focus on a 1996 agreement between New Zealand and the United Kingdom, the 2004 WCO Model Agreement and the 2015 Free Trade Agreement between New Zealand and South Korea.

In contrast, Part III discusses multilateral agreements for customs cooperation and highlights the 1997 Nairobi Convention, the 2003 Johannesburg Convention, a 2009 agreement between the ASEAN states, New Zealand and Australia and the 2013 agreement for the European customs information system called SIRENE.

In Part IV, some other information-sharing models are evaluated and the Five-Eyes, INTERPOL and PNRGOV systems are discussed in detail.

The terms of all the agreements that were examined were found to be unsuitable for sharing intelligence through the single window system. This Chapter identifies the typical shortcomings of the existing agreements.

## *I The Measures of Successful Legal Framework*

This Part collates the essential elements of a successful legal framework that were identified in the previous Chapters.

Chapter Two identified that intelligence is necessary to the trade risk-management that customs administrations perform for law enforcement and national security. Chapter Two also discussed the types of information that customs administrations might want to share and some of the preconditions necessary for that sharing to occur. The nature and form of this intelligence may change from time to time to meet the demands of changing technology, increased automation and the evolution of criminal methodologies. It was shown that, in order to promote trust between states, the legal framework must promote justice, mutual support and assistance while inhibiting manipulation by participating states. In order to do this, terms of the agreements should not be kept secret, even though the information that is shared must remain secret. Each state should be able to seek and receive assurance from those states with which it shares information that information is being accessed and used appropriately. There should also be self-reviews and audits for compliance with the rules for information-sharing.

Chapter Two showed that there must be sufficient autonomy for states to protect their citizens and other interests. States should be able to share information voluntarily: there should be no compulsion for states to share information. Chapter Two also demonstrated that it is important to ensure public confidence.

Chapters Two and Three discussed the duty of states to protect the content of intelligence and the identity of the sources of that intelligence. This is to ensure the safety of those sources and the confidentiality of sensitive investigation and intelligence methodologies. There must also be an appropriate balance between the competing needs of customs' duties of care, the need for overt compliance with international human rights laws and the need for secrecy. Accordingly, the legal framework must put rules in place to control the access and use of information. The rules must ensure information is kept only for as long as it is needed. There must also be self-reporting or at least independent review of compliance with these rules.

Public confidence can be improved by including clear terms that implement, as far as possible, the Privacy Principles of the OECD Privacy Framework discussed in Chapter Four. It was noted that the OECD Privacy Framework contains the most widely accepted

Privacy Principles. To promote public confidence, those Privacy Principles must be reflected in any legal framework that enables the sharing of personal information.

An individual's access to justice can be assured if terms exist to make certain that any intelligence used in an action against that individual can be disclosed and challenged in a judicial process. Chapter Four introduced a requirement for the state to take on an advocacy role for the individual when the existence of their personal information must be kept secret.[535] In the United Kingdom, special advocates are assigned to represent the interest of a suspect in closed proceedings for terrorism cases involving secret information.[536] The special advocate may be privy to secret information in closed legal proceedings, but he or she is prohibited from disclosing that information to the suspect.[537] Walker notes the effect of this advocacy for safeguarding the interests of the suspect is limited by factors such as restrictions on the advocates discussion with the subject once the secret information has been disclosed, an inability to call witnesses or independent experts and an absence of an instructing solicitor.[538]

Where the Privacy Principles are not fully implemented, facility should exist for the state to advocate on behalf of individuals or businesses. This advocacy will support individuals and businesses where the need for intelligence secrecy makes it difficult for them to complain or access justice. The state can assume responsibility for keeping personal information up to date and accurate, and deleted when no longer required, even though the information's existence may be kept secret from the subject of that personal information. This advocacy should not impede their right to begin proceedings of their own against a customs administration for a breach of their rights.

The advocacy by the state on behalf of the individual or business can be satisfied in part through the data controller role specified in the Accountability principle.[539] This advocacy role of the data controller differs from the special advocates established in the United Kingdom to represent a suspect's interests in a closed Court. The function of the data controller includes giving reassurance to the public that, although the information is kept secret, the processes that prevent abuses of personal information can be and are

[535] The proposed legal framework implements the Accountability principle through the establishment of a data controller, as discussed in Chapter Four.

[536] Terrorism Prevention and Investigation Measures Act 2011 (United Kingdom), Schedule 4 (10) and Clive Walker "The Reshaping of Control Orders in the United Kingdom: Time for a Fairer Go, Australia" (2013) 37 Melb U L Rev 143, at 178.

[537] In this context secret information means information for which the Court "considers that the disclosure of the material would be contrary to the public interest" this is set out in Terrorism Prevention and Investigation Measures Act 2011 (United Kingdom), Schedule 4 (4).

[538] Walker, above n 536, at 179 and Justice and Security Act 2013 (United Kingdom), s 9.

[539] OECD Privacy Framework, above n 12, at 15.

subject to scrutiny. Such advocacy will help states to meet the requirements of article 17 of the ICCPR, even though intelligence functions operate in an environment of secrecy.[540]

All of these requirements are summarised in the following table, which sets out the measures used to evaluate the information-sharing agreements discussed here.

**Table 4. Measures used to evaluate information-sharing agreements**

| Aim | Terms required |
|---|---|
| **Trust between states that intelligence is secured, accessed and used appropriately** | Information access and disclosure control<br>Audit, review or self-reporting of compliance<br>Information retention and destruction controls |
| **State autonomy** | Voluntary, not compulsory, information-sharing |
| **Include the Privacy Principles** | Collection Limitation<br>Data Quality<br>Purpose Specification<br>Use Limitation<br>Security Safeguards<br>Openness<br>Individual Participation<br>Accountability |
| **Promote access to justice, prohibit information gained through arbitrary search and seizure and prohibit information gained through torture** | Information is collected lawfully |
| **Implement intelligence-sharing through a single window** | Enables intelligence-sharing<br>Common standards/format for information exchange<br>Enables real-time electronic exchange |

## *II Bilateral Agreements*

This Part supports the thesis by demonstrating that existing bilateral agreements that enable customs administrations to share information, which can include intelligence, cannot meet the requirements for sharing intelligence through a single window system. It evaluates bilateral customs information-sharing agreements against the measures identified in Part I. Fifteen bilateral agreements, including a model agreement for customs cooperation, were analysed and assessed.[541] Agreements with the EU are treated as multilateral agreements because the EU is a single organisation representing multiple states. Table 5 lists the bilateral agreements that were analysed.

[540] ICCPR, above n 235, art 17.

[541] The term agreement is used here because not all these instruments are treaties. Many of these agreements are agreed at an organisational level, such as the Cooperative Arrangement between Customs Authorities, New Zealand – Hong Kong (1991) (not deposited, provided to the author by the New Zealand Customs Service) which was signed by the heads of the customs agencies.

**Table 5. Bilateral agreements assessed**

| *Year* | Party | Party | Type of agreement |
|---|---|---|---|
| *1991* | New Zealand | Hong Kong | Customs Cooperation.[542] |
| *1992* | New Zealand | South Korea | Customs Cooperation.[543] |
| *1996* | New Zealand | United Kingdom | Customs Cooperation.[544] |
| *1996* | New Zealand | United States | Customs Cooperation.[545] |
| *1997* | Japan | United States | Customs Cooperation.[546] |
| *1999* | United States | Columbia | Customs Cooperation.[547] |
| *2000* | United States | Mexico | Customs Cooperation.[548] |
| *2004* | WCO Model Agreement on Mutual Assistance in Customs Matters.[549] | | |
| *2005* | Japan | Canada | Customs Cooperation.[550] |
| *2006* | New Zealand | Australia | Customs Cooperation.[551] |
| *2007* | Japan | Indonesia | Economic Partnership.[552] |
| *2008* | New Zealand | China | Free Trade Agreement.[553] |

[542] Cooperative Arrangement between Customs Authorities, New Zealand – Hong Kong (1991) (not deposited, provided to the author by the New Zealand Customs Service).

[543] 1996 New Zealand – South Korea Agreement, above n 95.

[544] 1996 New Zealand – United Kingdom Agreement, above n 94.

[545] Cooperative Arrangement between Customs Authorities, New Zealand – United States of America (1996) (not deposited, provided to the author by the New Zealand Customs Service).

[546] Cooperative Arrangement between Customs Authorities, Japan – United States of America (1997), above n **Error! Bookmark not defined.**.

[547] Agreement Regarding Mutual Customs Assistance, United States of America – Colombia UST LEXIS 134 (1999).

[548] Customs Assistance Agreement, United States of America – Mexico UST LEXIS 258 (2000).

[549] WCO "Model Bilateral Agreement on Mutual Administrative Assistance in Customs Matters" (June 2004) (WCO Model Agreement) World Customs Organisation <www.wcoomd.org>.

[550] Border Services Agency Mutual Assistance Agreement, Japan – Canada (2005) (not deposited, retrieved from www.customs.go.jp/english/cmaa).

[551] Cooperative Arrangement between Customs Authorities, New Zealand – Australia (2006) (not deposited, provided to the author by the New Zealand Customs Service).

[552] Agreement between Japan and the Republic of Indonesia for an Economic Partnership UNTS 2780 I-48935 (2007).

[553] Free Trade Agreement between the Government of New Zealand and the Government of the People's Republic of China UNTS 2590 I-46123 101 (2008) (2008 New Zealand – China FTA).

| *Year* | Party | Party | Type of agreement |
|---|---|---|---|
| *2008* | Japan | Hong Kong | Customs Cooperation.[554] |
| *2010* | New Zealand | Hong Kong | Economic Partnership.[555] |
| *2015* | New Zealand | South Korea | Free Trade Agreement.[556] |

This is not an exhaustive list. These agreements were selected because of their accessibility and their broad geographic spread. They represent the terms accepted by ten countries across Asia, Europe, North America, Oceania and Central and South America; each having a different cultural context. This is important because, despite international conventions and treaties that refer to privacy or personal information, these terms and concepts take on different meanings in other cultures and societies.[557]

The sub-parts below contain a brief summary of 3 of the bilateral agreements examined. Included here are: the 1996 New Zealand – United Kingdom Agreement, salient because it implements privacy controls that are missing from many of the later agreements; the 2004 WCO Model Agreement, which is significant because it contains more of the measures than many other agreements, but it was not routinely implemented by WCO member states after it was made; and the 2015 New Zealand – South Korea FTA, because it implements more of the measures than an earlier customs cooperation agreement made between these states in 1992.

### *A New Zealand – United Kingdom 1996*

In 1996, the customs administrations of New Zealand and the United Kingdom agreed a cooperative arrangement.[558] This agreement is longer and more detailed than earlier New Zealand agreements with Hong Kong or Korea that were examined. This agreement has six paragraphs covering three pages under the heading "Communication of Information".[559] Seven of those paragraphs set out the types of information that may be shared.

[554] Customs Co-Operation and Mutual Administrative Assistance Agreement, Japan – Hong Kong (2008) (not deposited, retrieved from www.customs.go.jp/english/cmaa).

[555] New Zealand - Hong Kong, China Closer Economic Partnership Agreement UNTS 2479 I-48534 (2010) (2010 New Zealand – Hong Kong FTA) (2010 New Zealand – Hong Kong Agreement).

[556] Free Trade Agreement between New Zealand and the Republic of Korea (opened for signing 23 March 2015) (not deposited, retrieved from www.mfat.govt.nz) (2015 New Zealand – South Korea FTA).

[557] Barrington Moore *Privacy: Studies in Social and Cultural History* (ME Sharpe, Armonk NY, 1984), at ix.

[558] 1996 New Zealand – United Kingdom Agreement, above n 94

[559] Paragraphs 4–9.

Notable differences to the earlier Hong Kong and Korea agreements are the terms "to help ensure accuracy" in subsection 1 of paragraph 4:[560]

> 1. The customs authorities of the states will, upon request, supply to each other all information which may help to ensure accuracy in:
>    (a) the collection of customs duties and other import and export charges and, in particular, information which may help to assess the [value for revenue collection].
>    (b) the implementation of import and export prohibitions and restrictions;
>    (c) the application of rules not covered by other arrangements.

The scope of information and the wording of this paragraph allow the customs administrations to share information about suspected revenue fraud and smuggling. Paragraph 5 enables the customs administrations to share information about illegal movement of goods between the two states.[561] Paragraphs 6 and 7 allow the sharing of intelligence information as they specify information that is not necessarily linked to a specific import or export transaction. For example, paragraphs 6 and 7 allow the sharing of information about "persons known or suspected of contravening the customs laws of the other state" and "transactions, detected or planned". [562]

The need to ensure information is collected lawfully is not specified. There is only a statement that says assistance will be rendered in accordance with and subject to the laws of the state from which assistance is requested.[563]

This agreement enables the use of real-time electronic systems. It states "documents… may be replaced by computerised information produced in any form for the same purpose."[564] However, it confusingly goes on to say "files and documents which have been transmitted will be returned at the earliest opportunity".[565] That phrase makes sense in respect of physical copies of files as it implies the receiving customs administration will no longer hold the information. It makes no sense in respect of electronically supplied information. A return transmission will not ensure the information is removed from the electronic system that received it, meaning information could be retained for longer than it is needed and potentially used for purposes other than those that are set out in the agreement. These provisions do not satisfy the requirements of the Purpose

[560] Ibid.

[561] Paragraph 5.

[562] Paragraphs 6(a) and 7.

[563] Paragraph 2(2).

[564] Paragraph 8.

[565] Paragraph 9(2).

Specification Principle that sets out that information should be destroyed when it is no longer required.[566]

This agreement provides each state with broad reasons to withhold information, enabling each state to:[567]

> [withhold information where it] is considered to be prejudicial to the sovereignty, security, public order, public policy, or other essential interests...

The agreement has a page with the heading "Use of information and document". It has 2 paragraphs setting out how information will be used and protected. The first, paragraph 13, restricts the use of information to "the purposes of this arrangement".[568] It goes on to say that "[information]… will be accorded the same protection as is afforded to documents and information of like nature under the national law of that state".[569] Both states already had privacy laws in place that contained principles similar to the 1980 OECD privacy guidelines.[570]

Compared to other agreements examined for the period 1991 to 2000, the terms of this agreement are more suitable for use in the proposed legal framework. However, there is a lack of reference to common standards for electronic processing and no rules about how information is to be handled, processed and protected.

### *B WCO Model Agreement 2004*

In 2004 the WCO published a model bilateral agreement for mutual administrative assistance in customs matters. This document is substantial. It numbers 33 articles over 20 pages and has 42 pages of commentary. In regard to the purposes of information-sharing this model agreement has a general purpose of assisting the parties with:[571]

> … the proper application of customs law, for the prevention, investigation and combating of customs offences and to ensure the security of the international trade supply chain.

The 2004 Model Agreement specifies that the customs administrations that are party to the agreement shall provide each other information about: goods that are known to be the

---

[566] OECD Privacy Framework, above n 12, at 57 and Privacy Act 1993 (New Zealand), s6, principle 9.

[567] 1996 New Zealand – United Kingdom Agreement, above n 94, at para 15.

[568] Paragraph 13(1).

[569] Paragraph 13(2).

[570] Privacy Act 1993 (New Zealand), s 6, Data Protection Act 1984 (United Kingdom), at schedule 1 part 1, and OECD "OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data", above n 485, ss 50–62.

[571] WCO Model Agreement, above n 549, art 2(1).

subject of customs offences; means of transport; storage methods; persons known or suspected of committing an offence; whether goods have been unlawfully imported or exported; and "any other data that can assist customs administrations with risk-assessment for control and facilitation purposes".[572] The agreement allows the customs administrations to use automated processing systems for the exchange of information.[573] However, there is no reference to any common standards that are necessary for electronic information processing, such as the WCO Data Model.

The requirement for information to be collected only through lawful means is not addressed in this model agreement. There is however a statement that says "all assistance under this agreement by either contracting party shall be provided in accordance with its legal and administrative provisions".[574]

The 2004 Model Agreement has much clearer terms for the confidentiality of information and protecting privacy. Like other agreements discussed above, it says that information can be used only for the purposes set out in the agreement.[575] It states that customs administrations may not use information that has been shared with them for any other purpose, except with the permission of the customs administration that supplied the information.[576] The 2004 Model Agreement requires customs administrations to put in place protection for information that would satisfy the requirements of the national law of the customs administration that supplied the information.[577] It also states that in the absence of such protection personal data will be shared only when the customs administration that supplies the information is satisfied that the personal data will be appropriately protected where it is received.[578] The customs administration that receives personal data must inform the customs administration that supplies it of the use or uses to which that information has been applied.[579]

Personal data may only be kept for the time necessary to achieve the purpose for which it was supplied.[580] The customs administration that supplies the personal data is required to make sure that the information has been collected fairly and lawfully, that it is accurate

[572] Article 3.

[573] Article 6.

[574] Article 2(2).

[575] Article 24(1).

[576] Article 24(2).

[577] Article 25(2).

[578] Article 25(3).

[579] Article 25(4).

[580] Article 25(5).

and up to date and that it is not excessive in relation to the purposes for which it will be used.[581] Customs administrations are required to correct personal information without delay if it is found to be incorrect.[582] The 2004 Model Agreement requires each customs administration to put in place whatever security measures are necessary to protect the personal information it receives.[583] There is also a clause under which each customs administration accepts liability for the damage caused to a person through the customs administration's use of personal information.[584] That liability also applies to customs administrations that supply information that is inaccurate or that supply information "contrary to this agreement".[585]

Each customs administration is also required to keep a record of the personal information that it supplies or receives.[586] This last requirement would enable a customs administration to undertake an audit of the information that it has supplied to another customs administration. However, there are no provisions in 2004 Model Agreement to enable such an audit to take place

There is no requirement to collect personal information lawfully or with the knowledge or consent of the data subject. This does not satisfy the Collection Limitation principle, which requires that information should be obtained by lawful and fair means and with the knowledge or consent of the data subject.[587]

There is a requirement for each customs administration to notify a person within their territory of any decisions made within the scope of this agreement.[588] That provision goes some way towards the principle of Openness but it does not require a customs administration to notify that person if any information is held about them.[589] There is no provision that clearly sets out a framework for individuals to seek confirmation of or access to personal information held about themselves. For that reason, the Individual Participation principle has not been satisfied.[590]

---

[581] Article 25(6).

[582] Article 25(7).

[583] Article 25(9).

[584] Article 25(10).

[585] Ibid.

[586] Article 25(8).

[587] See Collection Limitation principle in Chapter Four.

[588] 2004 Model Agreement, above n 549, art 9.

[589] See Openness in Chapter Four.

[590] The Individual Participation principle specifies that a data subject should be able to enquire about and correct their personal information.

Nonetheless, the 2004 Model Agreement is superior to the bilateral agreements made before 2004 that were examined. It has better terms for the treatment of privacy and partially fulfils the requirements for automated information exchange through a single window. However, the terms of the 2004 Model Agreement do not appear to have been implemented in later agreements made for the same purpose. The reasons why other states have not implemented the terms of the 2004 Model Agreement would warrant further research.

### *C New Zealand – South Korea Free Trade Agreement 2015*

New Zealand made Free Trade Agreements with China in 2008, with Hong Kong in 2010 and with South Korea in 2015.[591] These three Free Trade Agreements are identical in the extent to which their terms meet the needs for sharing intelligence through a single window system. The 2015 New Zealand – Korea FTA is discussed below, as representative of these three agreements.

The customs cooperation terms in this FTA can be compared to the 1992 New Zealand – South Korea Agreement.[592] Chapter 4 contains articles 4.1–4.16 relating to customs procedures and trade facilitation. This agreement does not reflect the terms in the 2004 WCO Model Agreement. The chapter sets out the purposes for cooperation between the states as:[593]

> (a) the implementation and operation of the provisions of this Agreement…
> (b) the extent practicable, assisting each other in the tariff classification, valuation and determination of origin for preferential tariff treatment, of imported goods; and
> (c) other customs matters as the Parties may agree.

The phrase "other customs matters as the parties may agree" enables the customs administration of the two states to exchange information on virtually any matter permitted by their domestic law.[594] The 2015 New Zealand – Korea FTA is much less prescriptive than the 1992 New Zealand – Korea Agreement about the particular types of information that might be shared, such as "circumstances that may result in the commission of an offence". As in the 1992 New Zealand – Korea Agreement, the 2015 New Zealand – Korea FTA does not specify how this information is to be accessed, handled or used. Like the 2008 New Zealand – China FTA and the 2010 New Zealand –

[591] 2008 New Zealand – China FTA, above n 553; 2010 New Zealand – Hong Kong Agreement, above n, 555; and 2015 New Zealand – Korea FTA, above n 556.

[592] 1992 New Zealand – Korea Agreement, above n 95.

[593] Chapter 4 art 4.11(3).

[594] Section 281 of the Customs and Excise Act 1996 allows New Zealand Customs to disclose information to an overseas agency for a broad range of reasons.

Hong Kong FTA, the 2015 New Zealand – Korea FTA provides each state with the "essential security interests" as legitimate reasons to withhold information.[595] Also like the other FTAs, information classified as confidential by one party must be treated as such by the other and not disclosed without "specific written permission".[596]

In regard to the use of real-time electronic systems, the 2015 New Zealand – Korea FTA specifies "The customs administrations shall use information technology…".[597] It also refers to the WCO framework of standards including the WCO Data Model.[598]

The 2015 New Zealand – Korea FTA only refers to compliance with domestic privacy law as a reason for withholding information. There are no other stipulations about how personal information will be handled. Both parties to this agreement are OECD member states. Both states had privacy law in place at the time the agreement was made. [599]

Sharing information that has been obtained unlawfully by a third party is not specifically prohibited by this agreement.

The terms of this agreement are not suitable for widespread implementation for intelligence through a single window system. There is reference to electronic systems and the WCO standards. However, the agreement does not set out a robust framework for access to, handling of, or use of information. These omissions create uncertainty about how personal information will be handled, even though both states have privacy law in place. Nevertheless, this agreement makes significant advances towards suitability for single window intelligence purposes when compared to the 1992 New Zealand – South Korea Agreement.

### *D Summary of the Bilateral Agreements*

Most agreements that were examined provide opportunities for states to withhold information for various reasons ranging from "other substantial interests" and "essential interests" to "national security". In practice, those exceptions are likely to give the states significant leeway for withholding information. Each agreement has common purposes for sharing customs information: to facilitate trade and uphold or enforce customs law. Some agreements prevent the use of electronic systems to exchange information by requiring requests to be made in writing or orally. The later FTAs made by New Zealand enabled the use of electronic systems and refer to specific standards for the same.

[595] Chapter 20 art 20.2(1).

[596] Chapter 4 art 4.13(1).

[597] Chapter 4 art 4.5(2).

[598] Chapter 4 art 4.4.

[599] Public Agency Data Protection Act 1995 (South Korea) and Privacy Act 1993 (New Zealand).

However, no agreements discussed here set out terms for implementing the Privacy Principles. Some agreements contain neither direct nor indirect reference to privacy laws. In the case of the 2008 New Zealand – China FTA, the privacy references are one-sided as China had no privacy law in place at the time.[600]

None of the agreements had terms that are entirely suitable for a multilateral agreement for intelligence-sharing under a single window system. Overall, the terms in the 1996 New Zealand – United Kingdom Agreement and the FTAs New Zealand made with China, Hong Kong and Korea provide the best fit. However, the proposed legal framework needs explicit terms for securing and handling information to provide confidence that treaty partners will control information in a consistent manner.

Although the 2004 WCO Model Agreement has better terms for implementing the Privacy Principles, not all of the principles are fulfilled by the model agreement. The principle of Openness and Individual Participation are difficult to achieve if the information that is being shared and the means with which that information is collected must be kept secret from the subject of that information.

It is significant to note that the later agreements discussed here did not follow the 2004 WCO Model Agreement. It is difficult to identify any academic literature that identifies the reasons for this, so it warrants further study. It may be that one or both states did not have all of the institutions, such as a data controller, or procedures in place to be able to fulfil the privacy requirements. It could also be that the states that negotiated these later agreements determined that including the terms of the model agreement, especially the privacy terms, would have created bureaucracy and impeded an agreement being quickly reached. It is also possible that the state parties to these later agreements were unsupportive of the privacy controls. However, that seems unlikely. In each case the state parties to the agreements were members of the WCO that produced and endorsed the 2004 WCO Model Agreement.

Table 6 summarises the findings of all the bilateral agreements that were evaluated.

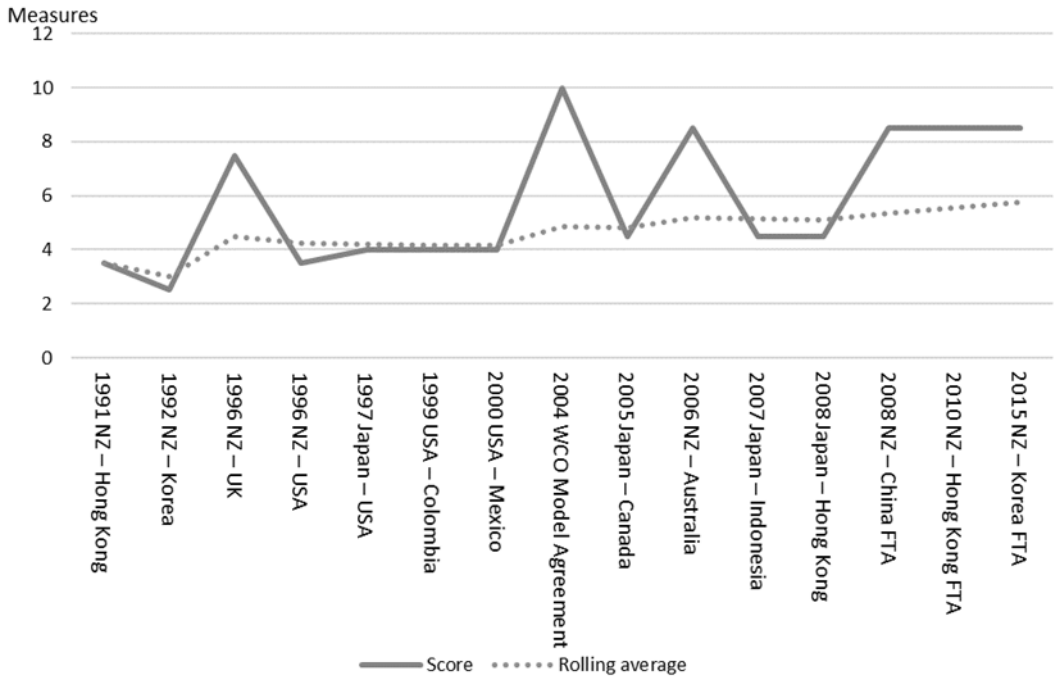
[600] In December 2012 China issued the Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Internet Information (Adopted at the 30th Meeting of the Standing Committee of the National People's Congress on December 28, 2012) (全国人民代表大会常务委员会关于加强网络信息保护的决定（2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过) (People's Republic of China), which sets out some general requirements for network services providers and business, but does not address privacy in the context of government administrative and law enforcement processes.

**Table 6. Summary of bilateral agreement assessments**

| *Theme* | Requirement | (✓) Meets, (P) Partially meets, or (✗) Fails to meet | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1991 NZ – Hong Kong | 1992 NZ – South Korea | 1996 NZ – UK | 1996 NZ – USA | 1997 Japan – USA | 1999 USA – Colombia | 2000 USA – Mexico | 2004 WCO Model Agreement | 2005 Japan – Canada | 2006 NZ – Australia | 2007 Japan – Indonesia | 2008 Japan – Hong Kong | 2008 NZ – China FTA | 2010 NZ – Hong Kong FTA | 2015 NZ – South Korea FTA |
| *Trust between states that intelligence is secured, accessed and used appropriately* | Information access and disclosure control | P | P | P | P | P | P | P | P | P | P | P | P | P | P | P |
| | Audit, review or self-reporting of compliance | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| | Information retention and destruction controls | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| | Information is held by each state, rather than stored in a single, central database (Big Data) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| *State autonomy* | Voluntary, not compulsory, information-sharing | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| *Include the Privacy Principles* | Collection Limitation | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | P | ✗ | ✗ | P | P | P |
| | Data Quality | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | P | ✗ | ✗ | P | P | P |
| | Purpose Specification | P | P | P | P | P | P | P | ✓ | P | P | P | P | P | P | P |
| | Use Limitation | P | P | P | ✓ | ✓ | ✓ | ✓ | ✓ | P | P | P | P | P | P | P |
| | Security Safeguards | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | P | ✗ | ✗ | P | P | P |
| | Openness | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | P | ✗ | P | ✗ | ✗ | P | P | P |
| | Individual Participation | ✗ | ✗ | P | P | ✗ | ✗ | ✗ | P | ✗ | P | ✗ | ✗ | P | P | P |
| | Accountability | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | P | ✗ | ✗ | P | P | P |
| *Promote access to justice, prohibit information gained through arbitrary search and seizure and prohibit information gained through torture* | Information is collected lawfully | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| *Implement intelligence-sharing through a single window* | Enables intelligence-sharing | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Common standards/format for information exchange | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ |
| | Enables real-time electronic exchange | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | P | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Figure 11 illustrates the extent to which each of these agreements have implemented the measures identified in Part I. Partially implemented measures have been assigned a score of 0.5 and fully implemented measures have been assigned a score of 1 for this comparison throughout this Chapter.

**Figure 11. Implementation of the measures in bilateral agreements**




The graph in Figure 11 shows that there has been a slight rise over time in the average number of measures that were implemented in this sample of bilateral agreements. A comparison of these agreements with multilateral agreements and other models for information-sharing is shown in a graph at the end of this Chapter.

Notably, the terms in the 2004 WCO Model Agreement were not uniformly implemented following its release. Over time, the agreements involving New Zealand generally increased the number of implemented measures, with the exception of the 1996 New Zealand – United States agreement. The measures implemented in the agreements involving the United States or Japan remained relatively constant in this sample.

## *III Existing and Past Multilateral Agreements*

This Part demonstrates that the multilateral agreements that enable customs administrations to share information, which can include intelligence, cannot meet the requirements for sharing intelligence through a single window system. It discusses past and existing approaches to sharing customs information through multilateral agreements. The multilateral agreements listed in the table below were reviewed.

**Table 7. Multilateral agreements assessed**

| *Year* | Parties | Type of agreement |
|---|---|---|
| *1977* | Albania, Algeria, Andorra, Australia, Austria, Bahrain, Belarus, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Chile, China, Croatia, Curacao, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hong Kong, Hungary, Ireland, Italy, Jordan, Kazakhstan, Latvia, Lithuania, Luxembourg, Madagascar, Mali, Malta, Mauritius, Moldova, Mongolia, Montenegro, New Zealand, Nigeria, Omar, Pakistan, Qatar, Russia, Saudi Arabia, Senegal, Seychelles, Slovakia, South Africa, Spain, Sweden, Switzerland, Tajikistan, Thailand, the former Yugoslav Republic of Macedonia, Trinidad and Tobago, Turkey, Ukraine, United Arab Emirates, United Kingdom, Zimbabwe and the EU member states. | Nairobi Convention.[601] |
| *1990* | EU and Andorra. | Customs Union Agreement.[602] |
| *1997* | EU and Canada. | Mutual assistance in customs matters.[603] |
| *1999* | EU and Uzbekistan. | Partnership and cooperation.[604] |
| *1999* | Belarus, Kazakhstan, Kyrgyzstan, Tajikistan and Russia | Customs union and common economic zone.[605] |

[601] Nairobi Convention, above n 114.

[602] Customs Union Agreement, European Union – Andorra OJ L374/13 (1990).

[603] Agreement on Customs Cooperation and Mutual Assistance, European Union – Canada OJ L 7/37 (1997).

[604] Agreement for Partnership and Cooperation, European Union – Uzbekistan OJ L229/1 (1999).

[605] Russian Federation and Belarus Customs Union UNTS 2212 I-39319 63 (2004); Agreement for Partnership and Cooperation, European Union – Kazakhstan OJ L196/1 (1999); Agreement for Partnership and Cooperation, European Union – Kyrgyz Republic OJ L196/46 (1999); Agreement for Partnership and Cooperation, European Union – Tajikistan OJ L350/1 (2009); Agreement for Partnership and Cooperation, European Union – Russia OJ L327/1 (1997); and Agreement on a Customs Union and Common Economic Zone, Belarus – Kazakhstan – Kyrgyzstan – Tajikistan – Russia UNTS 2212 I-39320 103 (26 February 1999).

| *Year* | Parties | Type of agreement |
|---|---|---|
| *2003* | WCO Member states | WCO Convention on mutual assistance (Johannesberg Convention).[606] |
| *2004* | EU and China. | Mutual assistance in customs matters.[607] |
| *2008* | EU and the Caribbean Forum (Antigua and Barbuda, Bahamas, Barbados, Belize, Grenada, Dominica, Guyana, Haiti, Jamaica, St Christopher and Nevis, St Lucia, St Vincent and the Grenadines, Suriname and Trinidad and Tobago). | Economic partnership between the EU and Forum of Caribbean States (CARIFORUM).[608] |
| *2009* | ASEAN (Cambodia, Indonesia, Lao, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam) and Australia and New Zealand. | ASEAN, Australia and New Zealand free trade area.[609] |
| *2012* | EU and Eastern and Southern Africa (Madagascar, Mauritius, Seychelles and Zimbabwe). | Mutual assistance in customs matters.[610] |

[606] International Convention on Mutual Administrative Assistance in Customs Matters (Johannesburg Convention) (opened for signing 27 June 2003) (deposited at the WCO, no document number, retrieved from www.wcoomd.org).

[607] Agreement on Mutual Administrative Assistance in Customs Matters, European Union – China OJ L 375/19 (2004).

[608] Economic Partnership Agreement, European Union – Antigua OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Barbuda OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Bahamas OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Barbados OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Belize OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Grenada OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Dominica OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Guyana OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Jamaica OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – St Christopher and Nevis OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – St Lucia OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – St Vincent and the Grenadines OJ L289/I/1 (2008); Economic Partnership Agreement, European Union – Suriname OJ L289/I/1 (2008); and Economic Partnership Agreement, European Union – Trinidad and Tobago OJ L 289/I/1 (2008).

[609] Agreement Establishing the ASEAN – Australia – New Zealand Free Trade Area UNTS 2672 I-47529 1 (opened for signing 27 February 2009).

[610] Protocol 2 for Mutual Administrative Assistance in Customs Matters, European Union – Madagascar OJ L111/1161 (2012); Protocol 2 for Mutual Administrative Assistance in Customs Matters, European Union – Mauritius OJ L111/1161 (2012); Protocol 2 for Mutual Administrative Assistance in Customs Matters, European Union – Seychelles OJ L111/1161 (2012); and Protocol 2 for Mutual Administrative Assistance in Customs Matters, European Union – Zimbabwe OJ L111/1161 (2012).

| *Year* | Parties | Type of agreement |
|---|---|---|
| *2012* | EU and Central American States (Colombia, Costa Rica, Panama, El Salvador, Nicaragua, Honduras and Guatemala). | Mutual assistance in customs matters.[611] |
| *2013* | SIRENE | A system established by the EU to enable 22 member states to target criminal nationals, goods and services that cross the internal borders of the member states.[612] |
| *2015* | Australia, Brunei Darussalam, Chile, Japan, Malaysia, Peru, Singapore, Vietnam, Mexico, Canada and New Zealand. | Trans-Pacific Partnership Agreement.[613] |
| *2015* | EU member states and New Zealand | Mutual assistance in customs matters.[614] |
| *2015* | EU member states | Mutual assistance and cooperation (the Naples II agreement).[615] |

These multilateral agreements include terms that were acceptable to more than half the member states of the United Nations. These multilateral agreements were assessed against the measures described in Part I.

The sub-parts below discuss three of the agreements that were analysed. The 1977 Nairobi Convention and its successor the 2015 Johannesburg Convention are significant

[611] Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Colombia OJ L354/2186 (2012); Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Costa Rica OJ L346/1902 (2012); Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Panama OJ L346/1902 (2012); Agreement for Mutual Administrative Assistance in Customs Matters, European Union – El Salvador OJ L346/1902 (2012); Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Nicaragua OJ L346/1902 (2012); Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Honduras OJ L346/1902 (2012); and Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Guatemala OJ L346/1902 (2012).

[612] Decision 2008/333/EC Adopting the SIRENE Manual and Other Measures for the Second Generation Schengen Information System (SIS II) [2008] OJ L123/1; Decision 2013/115/EU on the SIRENE Manual and Other Measures for the Second Generation Schengen Information System (SIS II) [2013] OJ L71/1; and Council Decision 2015/219/EU above n 113.

[613] Ministry of Foreign Affairs and Trade "Text of the Trans-Pacific Partnership" (2015) Ministry of Foreign Affairs and Trade <www.mfat.govt.nz>.

[614] Agreement between the European Union and New Zealand on Cooperation and Mutual Administrative Assistance in Customs Matters COM(2016) 17 final (not signed or ratified).

[615] Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on Mutual Assistance and Cooperation between Customs Administrations [1998] OJ C24/1 and Regulation 515/97 On Mutual Assistance between the Administrative Authorities of the Member States and Cooperation between the latter and the Commission to ensure the Correct Application of the Law on Customs and Agricultural Matters OJ L82/1.

because they were intended to implement a uniform framework for customs cooperation. The SIRENE system is included here because it was designed specifically for customs purposes.

### *A The Nairobi Convention 1977*

The first agreement examined here is the 1977 Nairobi Convention.[616] This agreement was ratified by 52 states, but it has never been widely accepted.[617] Under this agreement, all information submitted by contracting states is centrally pooled and administered by the WCO in Brussels and made available to all other contracting states.[618] The Nairobi Convention creates binding obligations for reciprocal cooperation between customs administrations. In the interviews discussed in Chapter Seven, one interviewee stated a belief that the binding obligations for a central pool of information administered by the WCO in Brussels were significant factors in the low rate of acceptance of the Nairobi Convention.[619]

The Nairobi Convention pre-dates the widespread use of electronic communications systems and databases. Pooling intelligence in a non-electronic format creates a risk that information will be retained for longer than it is needed. It also passes responsibility to a third party for authorising purposes and access to the information, meaning the customs administration that supplies the information has no control over that information.

The purpose of the Nairobi Convention is to enable the customs administrations of member states to assist each other in the prevention, investigation and repression of customs offences.[620] While it requires that information is used only for the purposes of the Nairobi Convention, it is silent on whether those uses include judicial proceedings. Customs administrations may make requests for assistance, including information, in writing.[621] There is no provision in the Nairobi Convention for using automated systems. A customs administration may assist the customs administration of another party to the

[616] Nairobi Convention, above n 114.

[617] Carsten Weerth "The Johannesburg Convention on Mutual Customs Assistance-is a new tool failing early?" (2016) 6(2) Customs Scientific Journal 35, at 35.

[618] Nairobi Convention, above n 616, Annex IX.

[619] Article 6 of the Nairobi Convention states that "[each] Contracting Party shall, subject to the laws and regulations in force in its territory, *take all necessary measures* to comply with a request for assistance" (emphasis assed). Reservations were originally not permitted by art 18 of the Nairobi Convention, but that article was amended in 1995 to permit reservations. See also Georg Dieter Gotschlich "The World Wide Developments of International Customs Law" 7 International Business LJ 947, at 951.

[620] Nairobi Convention, above n 114, art 2(1).

[621] Article 7(1).

Nairobi Convention on its own initiative.[622] It may also withhold assistance if it believes that to do so would "infringe upon [its state] sovereignty, security or other substantial national interests".[623] States may undertake enquiries or surveillance on behalf of and at the request of another state.[624] Each state is required to afford intelligence the same protection in respect of confidentiality and official secrecy that would be afforded to the same kind of information in its own territory.[625]

As noted above, the WCO is required to maintain a central pool of intelligence information "of international interest".[626] State Parties are able to supply conditions for handling and use with the information that they supply for the pool of information.[627] Extensive personal information is specified in the schedule of information to be provided to the WCO. It includes among other things: name; physical description; date of birth; address; related companies; nature of business and occupation.[628] The WCO is required to keep that central pool of information up to date and prepare summaries and studies on that information.[629] The Nairobi Convention is silent on how those summaries and studies are to be distributed, but it seems probable that they are to be made available to all parties to the Nairobi Convention through the non-electronic systems.

Although the WCO is required to keep the information up to date, there is no provision in the Nairobi Convention that requires the contracting states to notify the WCO of out of date, incomplete, or incorrect information.[630] Contracting states are entitled to request the deletion of information from the central pool of information.[631] However, there are no terms within the Nairobi Convention that ensure information is deleted when it is no longer required. In practice, it could be that contracting states supply expiry dates with the information that they submit. However, expiry dates are not included in the schedule of information types that the WCO expects to be submitted to the pool of information.[632] Consequently, it appears that the need to delete information when it is no longer required

[622] Annex I (1).

[623] Article 3.

[624] Annexes IV and V.

[625] Article 1(b).

[626] Annex IX (1).

[627] Annex IX (6).

[628] Annex IX (9).

[629] Annex IX (2).

[630] Annex IX.

[631] Annex IX (7).

[632] Annex IX, parts I – III.

has been overlooked. The only indirect reference to privacy law in the Nairobi Convention is a requirement that state parties provide assistance to other state parties "subject to the laws and regulations in force in its territory".[633] Neither the bilateral agreements discussed above, nor the Nairobi Convention explicitly prohibit the sharing of information that was collected unlawfully by a third party. There are no terms to require the recording of, voluntary reporting of, or independent audit of information-sharing and use.

This Nairobi Convention was designed for widespread implementation. It was written in 1977 which explains why automated systems were not indicated for information exchange, making this agreement hopelessly out-of-date.

The Nairobi Convention also predates many of the developments in privacy law including, among others: the EU Data Protection Directive; the OECD Privacy Framework; the New Zealand Privacy Act; the Australian Privacy Act; and the United Kingdom Data Protection Act.[634] Although the Nairobi Convention allows the WCO to update and amend the terms, the WCO has not made any updates to include the use of information systems such as single window or employ the common standards devised by the WCO.[635] The Nairobi Convention is unsuitable for sharing intelligence through a single window system because it requires information to be pooled centrally, does not enable real-time information sharing using electronic systems and lacks privacy controls.

### *B Johannesburg Convention 2003*

The Johannesburg Convention was made in 2003, but it is not in force as it has not been ratified by a sufficient number of contracting states.[636] It has only been ratified by three countries and a minimum number of five countries must ratify the agreement for it to come into force.

The Johannesburg Convention has a particular focus on information exchange and includes articles that set out rules for the treatment of personal information. Weerth, notes that, much like the 1977 Nairobi Convention, the Johannesburg Convention also imposes binding obligations for reciprocal cooperation on contracting parties – which may be a disincentive to ratification.[637] However, academic literature examining the reasons for

[633] Article 6(2).

[634] Directive 96/9/EC of the European Parliament and of the Council on the Legal Protection of Databases OJ L077; Directive 97/66/EC on the Protection of Privacy in the Telecommunications Sector OJ L24/1 (1997); OECD Privacy Framework, above n 12; Privacy Act 1993 (New Zealand); Privacy Act 1988 (Australia) and Data Protection Act 1998 (United Kingdom).

[635] WCO Data Model, above n 34.

[636] Johannesburg Convention, above n 606

[637] Weerth, above n 617, at 38.

the low rate of acceptance of the Nairobi and Johannesburg Conventions is scarce and this would warrant further research.

The Johannesburg Convention does, however, enable information exchange through a central database. It includes a Chapter on the protection of personal information within the central database, but it does not stipulate the process for information-sharing.[638] The Chapter includes privacy controls that limit the time that information may be stored in the database and the purposes for which it can be used.[639] There are also provisions that require information to be kept accurate and up to date.[640] However, the methods that are to be used to share information and to keep it accurate and up to date are not stated, meaning uniform methods still need to be discussed and agreed between the contracting states. Lack of clarity about the methods may be a disincentive for the ratification of this agreement.

There is a provision for an independent authority to verify that the information shared by the system is only retained for the time necessary to achieve the purpose for which it was supplied.[641] However, there are no other provisions enabling a state or central authority to audit the use or further disclosure of information that has been supplied to a state through the system.

The Johannesburg Convention does not reference the WCO Data Model or any other standards or formats for information-sharing. This means further discussion and agreement between contracting states would be needed to enable information to be shared.

Although the Johannesburg Convention implements most of the established measures discussed in Part I of this Chapter, there are few provisions that implement the degree of accountability and transparency required by the proposed legal framework. The lack of clarity regarding the methods that will be used to share information and implement the privacy controls, along with the lack of data standards make the Johannesburg Convention unsuitable for sharing customs intelligence through a single window system.

### *C SIRENE System 2013*

In 2007 the EU established the second-generation Schengen Information System (SIS II) for use by 22 EU members of the Schengen Area.[642] The Supplementary Information

[638] Johannesburg Convention, above n 606, Chapter X.

[639] Articles 37 and 38(2).

[640] Articles 39 and 40.

[641] Article 37(4).

[642] Decision 2007/533/JHA, above n 21.

Request at the National Entries (SIRENE) system became operational in 2013.[643] The system enables member states to identify and intervene with people, goods and craft that contravene customs laws when crossing the borders between the states.[644] Real-time intelligence-sharing is possible within the SIRENE system and specific data formats are specified. The rules of the system also comply with the Privacy Principles. However, a participating state may withhold information to protect other law enforcement activities and the rights of third parties. The SIRENE system shares information through a centralised database, administered by the EU Agency for large-scale IT systems (EU-LISA), and a bureau service that is accessible by all member states.[645] Consequently, control of access to secret information could be problematic, the use of a centralised database is unsuitable for the proposed legal framework.[646]

The Schengen Area member states are the EU Member states, except Bulgaria, Croatia, Cyprus, Ireland, Romania and United Kingdom.[647] Five countries signed the Convention Implementing the Schengen agreement on 19 June 1990.[648] The Schengen agreement allows all nationals, goods and services to cross the internal borders of member states freely.[649]

The SIRENE system was set up to be a common information system allowing competent authorities of the member states to cooperate by sharing information. Those competent authorities are laid down as:[650]

> (a) authorities responsible for border controls…
> (b) authorities carrying out and coordinating other police and customs checks…
> (c) national judicial authorities and their coordination authorities;
> (d) authorities responsible for issuing visas… residence permits… [and the administration of] third country nationals…

---

[643] Ibid and Council Decision 2015/219/EU, above n 113, at 75. See also European Commission "SIRENE cooperation" (10 November 2017) European Commission <ec.europa.eu>.Confusingly, the French directory of companies is also called SIRENE at Insee "Contents of the Sirene Database" (11 November 2017) Insee <www.sirene.fr>.

[644] See Council Decision 2015/219/EU, above n 113, at 84.

[645] EU-LISA is administered in Tallinn, Estonia and operations are based in Strasbourg, France. See European Commission "Alerts and data in the SIS" (10 November 2017) European Commission <ec.europa.eu> and European Commission "Agencies" (10 November 2017) European Commission <ec.europa.eu>.

[646] Discussed in Part I of Chapter Four.

[647] European Commission "Schengen Information System" (2015) European Commission <ec.europa.eu>.

[648] Decision Bringing Into Force the Convention Implementing the Schengen Agreement of 19 June 1990 [2000] OJ L239/19.

[649] Council Decision 2015/219/EU, above n 113, at 82.

[650] Ibid.

(e) authorities responsible for issuing vehicle registration certificates…

The SIRENE system contains information to help identify a person or object and the necessary action to be taken.[651] The SIRENE Manual sets out all the rules and procedures for the use of the SIRENE system[652]. It is possible for information to be duplicated in the SIRENE and INTERPOL databases. The Manual states that the SIRENE system is not to replace or replicate the role of INTERPOL, "although tasks may overlap".[653] The SIRENE Manual says that alerts requiring action that are placed on the SIRENE system always take priority over alerts requiring action that are placed on the INTERPOL system.[654] Every piece of information entered into SIRENE is associated with an alert. Each alert indicates an action must be taken. The actions and priority for alerts on persons are as follows:[655]

(a) arrest with a view to surrender or extradite;
(b) refuse entry;
(c) place under protection;
(d) specific check for immediate action (is committing, or intends to commit an offence);
(e) specific check (other);
(f) discrete check for immediate action (is committing, or intends to commit an offence);
(g) discrete check (other); and
(h) communicate whereabouts.

The actions and priorities on alerts for "objects" (including traded goods) are:[656]

(a) use as evidence;
(b) seizure specific check for immediate action (is being used to commit, or intended to use to commit an offence);
(c) specific check (other);
(d) discrete check for immediate action (is being used to commit, or intended to use to commit an offence); and
(e) discrete check (other).

[651] At 84.

[652] Decision 2008/334/JHA Adopting the SIRENE Manual and Other Measures for the Second Generation Schengen Information System (SIS II) [2008] OJ L123/39 and Decision 2008/333/EC, above n 612.

[653] Council Decision 2015/219/EU, above n 113, at 85.

[654] Ibid.

[655] At 92 and Decision 2007/533/JHA, above n 21, art 36.

[656] Council Decision 2015/219/EU, above n 113, at 92.

The format for data exchanged electronically within the SIRENE system is prescribed by a companion document called "Data exchange between SIRENE Bureaux".[657] The SIRENE bureau of each member state is required to maintain the accuracy of data.[658] A member state which finds incorrect information in the SIRENE system must inform the member state that supplied the information so that it can be corrected within 10 calendar days.[659] Each member state is also required to implement a national Data Quality audit.[660] The rules specify that personal data "shall be kept only for such time as may be required to achieve the purposes for which they were supplied" and must then be immediately deleted.[661] The processing of personal data within SIRENE must comply with the European data protection rules.[662] Individuals are able to request access to any information in the SIRENE system about themselves.[663]

However, unlike the INTERPOL system:[664]

> Information shall not be communicated to the data subject if this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights and freedoms of third parties.

The rules concerning the collection and use of data are specific. There are also provisions that allow the use of information within the SIRENE system for other purposes as long as prior authorisation has been granted by the member state that supplied the information. However, there are no rules that prevent a state from entering information which has been collected unlawfully into the SIRENE system.

The rules of the SIRENE system are superior to any other implemented agreements or systems that were examined in respect of suitability for sharing customs intelligence via a single window system. Intelligence-sharing is possible within the system. Specific formats for information exchange are mandated. There are controls within the system for personal information that comply with the Privacy Principles. However, those controls provide an ability for the state to withhold information to protect other law enforcement activities and the rights of third parties. There are controls to make sure that information

[657] At 86.

[658] At 88 and 97.

[659] At 97.

[660] Ibid, at 88.

[661] Ibid.

[662] Decision 2007/533/JHA, above n 21, art 57.

[663] Article 58(1).

[664] Article 58(4). The terms for the INTERPOL system, which enable any person to access information about themselves which is held in the system, are discussed in Part IV of this Chapter.

is kept up to date, used only for specific purposes, and deleted when no longer required. There is also a requirement to regularly audit the quality of data. The scope of that audit could be improved to ensure the SIRENE system is used appropriately. Otherwise, the only significant drawbacks of this system are that it requires information to be stored in a central database that is accessible by all member states and it is not designed for real-time transaction processing. Broad access by all member states reduces the secrecy of the information contained within the system, making this approach unsuitable for the proposed legal framework.

### *D Summary of the Multilateral Agreements*

The majority of the multilateral agreements that were examined are between states or groups of states and the EU. The multilateral agreements were selected because of their accessibility and their broad geographic spread. The agreements are for customs unions, customs mutual assistance or partnership, economic partnership, or free trade. Each agreement includes an element of customs cooperation and the sharing of customs information.

The multilateral agreements that include the EU benefit from the negotiating power the EU has over the smaller states or groups of states that comprise the other party. That negotiating power should have allowed the EU to ensure its privacy requirements are implemented by the smaller states. The EU Data Protection Directive requires that information transmitted to non-EU states is afforded the same protection as it is within the EU.[665] As discussed in Chapter Four, the EU Privacy Principles are very similar to the Privacy Principles of the OECD Privacy Framework. The European Commission takes part in the work of the OECD and, while not a full member, its participation is more than that of an observer.[666]

It appears that the EU has used a consistent set of terms for establishing its customs cooperation agreements after 1997. Those agreements use a standard clause requiring personal information to be protected in the same way that it is in the state that provides that information. On the face of it, that clause requires non-EU states to apply the Data Protection standard of care to personal information they receive from the EU. Of course, the EU is required to protect information as per the Data Protection Directive at a minimum.[667] This happens even if the state from which it receives personal information has no privacy laws. However, this clause on its own will not achieve the outcomes intended by the Data Protection Directive. To achieve those outcomes, explicit terms must state how the Privacy Principles will be implemented. For example, unless the agreements

[665] Directive 96/9/EC, above n 634, at [66].

[666] OECD "Members and Partners" (2015) OECD <www.oecd.org>.

[667] Directive 96/9/EC, above n 634.

establish a data controller and rules for recording access to and use of personal information shared under the agreement, it is unlikely that the principle of Accountability will be understood and implemented. Similarly, information will not be kept up to date and accurate, as required by the Data Quality principle, unless there are terms in these agreements that set out how this is to happen. All of these requirements could have been implemented easily in agreements such as the EU – Canada 1997 agreement where all parties were OECD members and had privacy law that aligned with the OECD Privacy Guidelines.

There are no specific terms for implementing the Privacy Principles in the agreements between Australia, New Zealand and the ASEAN states. There is no reference to information-sharing or privacy in the agreement between Belarus, Kazakhstan, Kyrgyzstan, Tajikistan and Russia. These omissions could be due to an intention not to share intelligence information (including personal information), an intention to work out terms for sharing personal information through further negotiation, or to a lack of regard for privacy rights generally. In the case of the Australia, New Zealand and the ASEAN states agreement, the first or second scenarios seem more likely as both Australia and New Zealand are members of the OECD and had privacy laws in place. There is no reference in the ASEAN agreement to the types of intelligence that could be used for risk-management, such as information about suspicious goods or persons, so it seems most likely that Australia, New Zealand and the ASEAN states did not intend to share this intelligence under this agreement.

The SIRENE system implements most of the measures identified in Part I of this Chapter. However, the SIRENE system was not designed for real-time transaction and risk-management processing and it implements a single, central database that every member state can access and use. This creates Big Data privacy concerns and issues of trust in relation a central database, as discussed in Chapter Two and Chapter Four.

In addition to lacking terms to implement the Privacy Principles, most of the agreements lacked terms and standards for electronic information-sharing. Because the terms and standards are not included in these agreements, they would need to be negotiated separately. The terms of all these multilateral agreements need elaborating in order to be useful for a legal framework for sharing intelligence through a single window system. It is asserted here that it is essential to include clear terms for implementing the Privacy Principles and the other requirements that would ensure confidence for intelligence-sharing.[668]

Table 8 summarises the assessment of all the multilateral agreements that were examined.

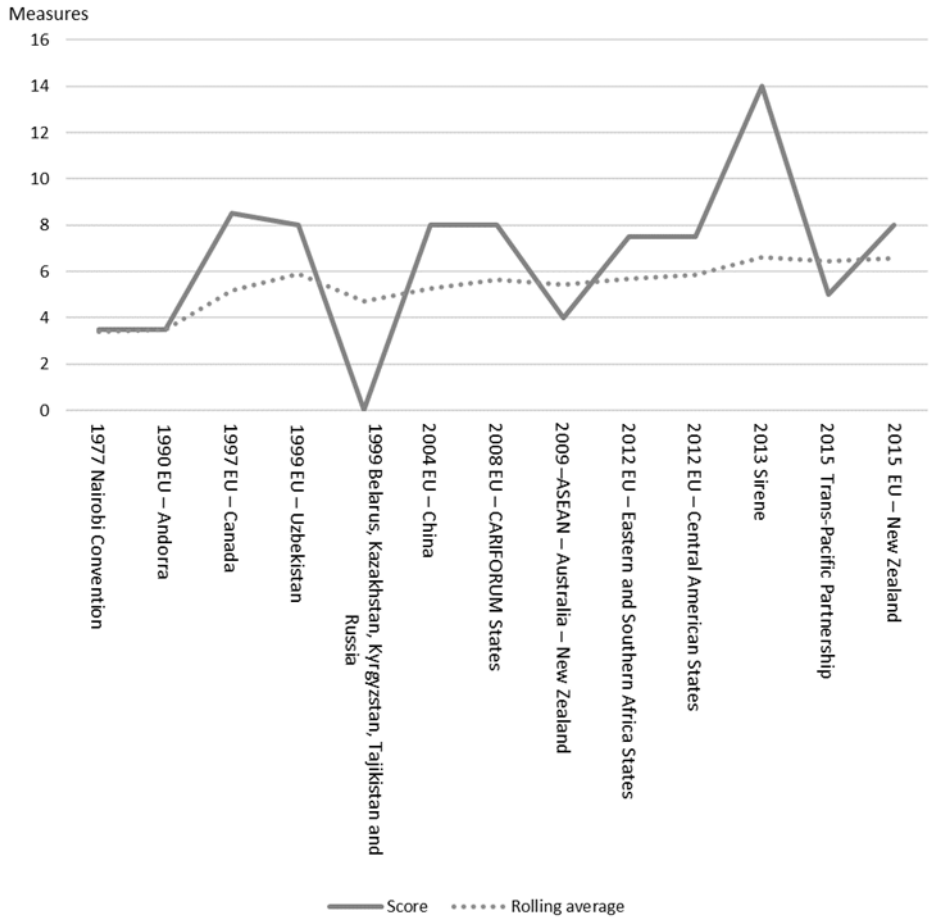
[668] Ministry of Foreign Affairs and Trade "Text of the Trans-Pacific Partnership" Ministry of Foreign Affairs and Trade (2015) <www.mfat.govt.nz>.

**Table 8. Summary of multilateral agreement assessments**

| *Theme* | Requirement | 1977 Nairobi Convention | 1990 EU – Andorra | 1997 EU – Canada | 1999 EU – Uzbekistan | 1999 Belarus, Kazakhstan, Kyrgyzstan, Tajikistan and Russia | 2003 Johannesburg Convention | 2004 EU – China | 2008 EU – CARIFORUM States | 2009 ASEAN – Australia – New Zealand | 2012 EU – Eastern and Southern Africa States | 2012 EU – Central American States | 2013 SIRENE | 2015 Trans-Pacific Partnership | 2015 EU – New Zealand | 2015 EU members (NAPLES II) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | (✓) Meets, (P) Partially meets, or (✗) Fails to meet | | | | | | | | | | | | | | |
| *Trust between states that intelligence is secured, accessed and used appropriately* | Information access and disclosure control | P | P | P | P | ✗ | P | P | P | P | P | P | ✓ | ✗ | ✓ | P |
| | Audit, review or self-reporting of compliance | ✗ | ✗ | ✗ | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| | Information retention and destruction controls | ✗ | ✗ | ✗ | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ |
| | Information is held by each state, rather than stored in a single, central database (Big Data) | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ |
| *State autonomy* | Voluntary, not compulsory, information-sharing | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | P | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| *Include the Privacy Principles* | Collection Limitation | ✗ | ✗ | P | P | ✗ | P | P | P | ✗ | P | P | P | ✗ | ✗ | P |
| | Data Quality | ✗ | ✗ | P | P | ✗ | P | P | P | ✗ | P | P | ✓ | ✗ | ✗ | ✓ |
| | Purpose Specification | P | P | P | P | ✗ | P | P | P | P | P | P | ✓ | ✗ | ✓ | ✓ |
| | Use Limitation | P | P | P | P | ✗ | P | P | P | P | P | P | ✓ | ✗ | ✓ | ✓ |
| | Security Safeguards | ✗ | ✗ | P | P | ✗ | P | P | P | ✗ | P | P | ✓ | ✓ | ✓ | P |
| | Openness | ✗ | ✗ | P | P | ✗ | ✗ | P | P | ✗ | P | P | ✓ | ✗ | ✗ | P |
| | Individual Participation | ✗ | ✗ | P | P | ✗ | ✗ | P | P | ✗ | P | P | ✓ | ✗ | ✗ | ✓ |
| | Accountability | ✗ | ✗ | P | P | ✗ | ✗ | P | P | ✗ | P | P | ✓ | ✗ | ✗ | P |
| *Promote access to justice, prohibit information gained through arbitrary search and seizure and prohibit information gained through torture* | Information is collected lawfully | ✗ | ✗ | P | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | P | ✗ | ✗ |
| *Implement intelligence-sharing through a single window* | Enables intelligence-sharing | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | P | ✓ | ✓ | ✓ |
| | Common standards/format for information exchange | ✗ | ✗ | P | P | ✗ | ✗ | P | P | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ |
| | Enables real-time electronic exchange | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | P | ✓ | ✗ |

Figure 12 illustrates the extent to which each of these multilateral agreements have implemented the measures identified in Part I.

**Figure 12. Implementation of the measures in multilateral agreements**




The graph in Figure 12 shows that there has been a slight rise over time in the average number of measures that were implemented in the multilateral agreements examined here. A graph at the end of this Chapter compares these agreements with bilateral agreements and other models for information-sharing and shows the overall trend.

Notably, the 2013 agreement for the SIRENE system in Europe implemented almost all of the measures and none were implemented in the 1999 agreement between Belarus, Kazakhstan, Kyrgyzstan, Tajikistan and Russia. The agreements involving the EU generally implemented more of the measures than the other agreements

## *IV Other Information-sharing Agreements*

This Part examines other models for information sharing to illustrate the extent to which these other models typically meet the requirements for sharing intelligence through a single window system. It assesses them against the measures identified in Part I. Detailed analysis was undertaken of the six models for information-sharing listed in Table 9. This is not an

exhaustive list of international information-sharing models. The Five-Eyes, INTERPOL and PNRGOV agreements were selected for discussion in this part because of their role in law enforcement and security practices. Although the PNRGOV system is a commercially-accessible system and it is not used for the exchange of law enforcement or security information, it was selected because it is used by customs administrations in risk-management processes.

**Table 9. Other information-sharing models assessed**

| *Year* | Name | Purpose |
|---|---|---|
| *1947* | Five Eyes.[669] | An intelligence-sharing agreement between the United States, the United Kingdom, Canada, Australia and New Zealand for national security purposes. |
| *1956* | INTERPOL.[670] | An agreement between 190 member states to enable mutual assistance between their police authorities. |
| *1989* | Financial Action Task Force.[671] | A body comprising 34 member states and regional authorities to combat money laundering, the financing of terrorist activities and other threats to the integrity of the International Finance system. |
| *1996* | Europol.[672] | A Europe-based system between EU members to enable mutual assistance between their police authorities. |
| *2010* | Foreign Account Tax Compliance Act.[673] | A system established by the United States, through agreements with 77 other states, to target tax non-compliance by United States taxpayers with foreign accounts. |
| *2013* | PNRGOV.[674] | An initiative of the WCO, IATA and the International Civil Aviation Organisation (ICAO) to ensure passengers have valid travel documentation and to assist states to risk-assess passengers and their baggage. |

669 National Security Agency "Revision of the UKUSA Agreement" (2 September 1954) National Security Agency <www.nsa.gov> and National Security Agency "Terms of Reference for Negotiating a New COMINT Agreement, 2 September 1954: Memorandum for the Members of USCIB" (21 December 1954) National Security Agency <www.nsa.gov>.

670 INTERPOL "Constitution of the ICPO-INTERPOL I/CONS/GA/1956(2008)" (2008) INTERPOL <www.interpol.int>.

671 United Nations Office on Drugs and Crime "UN Instruments and Other Relevant International Standards on Money-Laundering and Terrorist Financing" (2015) United Nations Office on Drugs and Crime <www.unodc.org>; Convention for the Suppression of the Financing of Terrorism UNGA Res 54109 (9 December 1999); Convention Against Corruption UNGA Res 5/84 (31 October 2003) and Convention Against Transnational Organized Crime UNGA Res 55/25 (15 November 2000).

672 Regulation 2016/794, above n 20.

673 United States Department of the Treasury "Foreign Account Tax Compliance Act (FATCA)" (15 May 2017) United States Department of the Treasury <www.treasury.gov>; Double Tax Agreements (United States of America - FATCA) Order 2014/209 (New Zealand); FATCA Agreement Model 1A IGA Reciprocal, Preexisting TIEA or DTC, 30 November 2014 (retrieved from www.treasury.gov) (United States); and, for example, Agreement between the Government of the United States of America and the Government of the Republic of Korea to Improve International Tax Compliance (2015) (not deposited, retrieved from www.treasury.gov) and Convention between the Government of the French Republic and the Government of the United States of America for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income and Capital UNTS 1963 I-33537 (31 August 1994).

674 WCO "Guidelines on Advance Passenger Information (API)" (October 2014) WCO <www.wcoomd.org>.

The sub-parts below briefly summarise the Five-Eyes, INTERPOL and PNRGOV agreements.

### *A Five Eyes 1947*

The first agreement examined here is the Five Eyes agreement made in the post-World War II period. This agreement is significant because it reflects the secrecy of the early Cold War period and it does not provide for information exchange via the computerised systems that were to develop later.

The Five Eyes agreement was established for sharing national security intelligence, particularly communications intelligence (COMINT), after World War II.[675] Almost all the Five Eyes terms relating to how information is transferred, accessed, used and managed remain secret.[676] That secrecy is not conducive to public confidence or acceptance and implementation by other states. Because of the secrecy surrounding the Five Eyes agreement, its terms cannot be analysed in detail. Moreover, the details of the agreement that have been declassified show that the arrangement is focussed on sharing the product of intercepted foreign communications and not information from other sources of intelligence.

Information in this Part has been obtained from declassified documents made available through the United Kingdom National Archives and other sources. A number of documents that provide more background on the nature of the Five Eyes relationship were illegally disclosed by Edward Snowdon in 2013 and reported by Greenwald.[677] No information from those illegally disclosed documents has been included here because the documents have not been declassified and verified by the relevant governments.

The UKUSA agreement, as the Five Eyes agreement was first known, was established between the United Kingdom and the United States in 1946 to enable the sharing of signals

[675] National Security Agency "Revision of the UKUSA Agreement" National Security Agency (2 September 1954) <www.nsa.gov> and National Security Agency "Terms of Reference for Negotiating a New COMINT Agreement, 2 September 1954: Memorandum for the Members of USCIB" National Security Agency (21 December 1954) <www.nsa.gov> for more detail.

[676] For more detail see National Security Agency "UKUSA Agreement Release 1940-1956 " (24 June 2010) National Security Agency <www.nsa.gov>, or National Archives "Newly Released GCHQ Files: UKUSA Agreement" (June 2010) The National Archives <www.nationalarchives.gov.uk> for access to the declassified documents.

[677] Glenn Greenwald "NSA Collecting Phone Records of Millions of Verizon Customers Daily" *The Guardian* (online edition, London, 6 June 2013); Mirren Gidda "Edward Snowden and the NSA files – Timeline" *The Guardian* (online edition, London, 22 June 2013) and Joshua Eaton "Timeline of Edward Snowden's Revelations" (5 June 2013) Al Jazeera <america.aljazeera.com>.

intelligence in the Cold War era following World War II.[678] New Zealand and Australia formally became parties to the Five Eyes agreement in 1955.[679] The objective of the Five Eyes agreement can be inferred from the General Principles of Security and Dissemination:[680]

> … while the following principles are in general of universal application, certain of those primarily applicable to peacetime must be modified in time of war or emergency, to ensure that the maximum operational benefit consistent with security is derived from the source.

From that text it can be inferred that the overall objective of the Five Eyes agreement is "security". Although the term security is not defined in the declassified Five Eyes documents, since the agreement arose out of the parties' World War II collaboration it can be assumed that security in this context meant defensive security against potentially hostile forces.

Access to information is permitted on a "need-to-know" basis for individuals "who require it in the performance of their duties".[681] Parties to the agreement are able to withhold information when required by their "special interests".[682] The term "special interests" is not defined in the declassified documents. It can be expected that sovereign requirements will always take precedence over other interests. For example, a drug trafficker turned around at the New Zealand border is a desired outcome with no consequences for New Zealand. However, the return of that drug trafficker may lead to capital punishment in the originating state. Therefore, New Zealand might not provide information about the drug offence to the originating state as to do so could make New Zealand complicit in capital punishment.[683]

---

[678] Derek S Reveron "Old Allies, New Friends: Intelligence-Sharing in the War on Terror" (2006) 50(3) Orbis 453, at 454 and 455.

[679] Declassified NSA and GCHQ document "Amendment No.4 to the Appendices to the UKUSA Agreement (Third Edition) (HW80/11)" (10 May 1955) <www.nationalarchives.gov.uk>, Appendix J s 7.

[680] National Archive "Tabular Comparison of 1946 and 1948 Appendices to the US-British Communication Intelligence Agreement (HW80/8)" (1948) United Kingdom National Archives <www.nationalarchives.co.uk>, at 1948 Appendix B Introduction (2).

[681] At 1948 Appendix B (12).

[682] National Archives "British-US Communication Intelligence Agreement (HW80/4)" (5 March 1946) United Kingdom National Archives <www.nationalarchives.gov.uk>, s 4(b).

[683] The possibility of a death penalty is a reason for the New Zealand government to deny assistance to the law enforcement agency of another state in Mutual Assistance in Criminal Matters Act 1992 (New Zealand), s 27(2).

The purpose of the agreement in 1955 was:[684]

> … the exchange of the [intelligence] following operations relating to foreign communications:–
>
> 1. Collection of traffic.
> 2. Acquisitions of communications documents and equipment.
> 3. Traffic analysis.
> 4. Cryptanalysis.
> 5. Decryption and translation.
> 6. Acquisition of information regarding communications, organisations, procedures, practices and equipment.

It is uncertain to what extent the purpose and scope of the Five Eyes agreement has changed since 1955.[685] It can be assumed that the scope of intelligence collection has increased since the development of digital communications, computer systems and the Internet. Reveron argues that the scope of this relationship has expanded significantly following the 9/11 terrorist attacks and the start of the "war on terror".[686] Walsh and Miller note that:[687]

> The tension between the legitimate collection of information for national security and the rights to privacy of the individual" has in liberal democratic states has increased markedly since 9/11.

Sir Stephen Lander, former United Kingdom Director-General of the Security Service, notes that the focus of the United Kingdom's participation in the Fives-Eyes arrangements has evolved and now probably includes:[688]

> - international terrorism, and the whereabouts, capabilities
> - and intentions of [Al Qaeda] members in particular;
> - heroin and cocaine smuggling, people, routes and methods;
> - weapons of mass destruction (WMD) programmes and plans;
> - terrorism associated with Northern Ireland;
> - the Middle East peace process;
> - the security situation in Iraq and Afghanistan; ….

[684] "Amendment No.4 to the Appendices to the UKUSA Agreement (Third Edition) (HW80/11)", above n 679, s 4; National Archives "Outline of Draft British-US Communication Intelligence Agreement (HW80/2)" (1 November 1945) United Kingdom National Archives <www.nationalarchives.gov.uk>, s 3(a) and National Archives, above n 682, s 3.

[685] Paul Farrell "History of 5 Eyes – Explainer" *The Guardian* (online edition, London, 2 December 2013).

[686] Reveron, above n 678, at 460.

[687] Patrick F Walsh and Seumas Miller "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden" (2016) 31(3) Intelligence and National Security 345, at 345.

[688] Sir Stephen Lander "International Intelligence Cooperation: An Inside Perspective" (2004) 17(3) Cambridge Review of International Affairs 481, at 481 and 483.

There are no references to other national law or privacy in the declassified agreement. Walsh and Miller note:[689]

> In some such contexts, e.g. organized crime, protocols (indeed, laws) are well-developed. Other contexts are bereft of protocols and subject only to vague and very permissive legislation.

There are similarly no terms in the declassified agreement that prohibit the sharing of unlawfully obtained information. Many parts of the declassified agreement have been redacted.[690] The entire agreement has been shrouded in secrecy, as evidenced by a statement within the declassified versions saying:[691]

> It will be contrary to this agreement to reveal its existence to any third party unless otherwise agreed by the two parties.

This is consistent with the position of successive governments until 1983, when the Prime Minister of the United Kingdom, declared as an exercise of royal prerogative that employees of the United Kingdom Government Communications Headquarters (GCHQ) could not join a trade union. The Council of Civil Service Unions sought a judicial review and the case went to the House of Lords.[692] Prior to 1983, the government did not acknowledge the existence of GCHQ.

A privacy charity called Privacy International claims that the secret details of the Five Eyes should be published. It says:[693]

> The UK government's GCHQ monitoring service invoked a blanket exemption that excuses it from any obligation to be transparent about its activities to the British public.

Such secrecy prevents an analysis of whether adequate terms are in place for implementing the Privacy Principles. This lack of transparency reduces public confidence in the state's collection and use of personal information. There has been substantial recent media attention

[689] Walsh and Miller, above n 687, at 349.

[690] For example, see pages 26, 31, 37 and 42 of Declassified NSA and GCHQ document "Amendment No.4 to the Appendices to the UKUSA Agreement (Third Edition) (HW80/11)", above n 684.

[691] National Archives, above n 682, at 5(a) and "Amendment No.4 to the Appendices to the UKUSA Agreement (Third Edition) (HW80/11)", above n 684, at 6(a).

[692] *Council of Civil Service Unions and Others v Minister for the Civil Service* [1983] UKHL 6, [1985] AC 374, [1984] 3 WLR 1174, [1985] ICR 14, [1984] 3 All ER 935, [1985] IRLR 28.

[693] Owen Bowcott "'Five Eyes' Surveillance Pact Should be Published, Strasbourg Court Told" *The Guardian* (online edition, London, 9 September 2014).

to the Five Eyes agreement due to concern about this secrecy.[694] In this regard, two cases were taken in 2014 to the United Kingdom Investigatory Powers Tribunal, regarding the interception of the claimants' personal or legally privileged information by the security services.[695] In both cases the complainants alleged the security services breached arts 8 and 10 of the European Convention of Human Rights. The Tribunal decided that, prior to the disclosures in question, the interception regime of the security services did contravene arts 8 or 10. The security services were ordered to updated their policies and procedures in light of a new Interception Code of Practice.[696]

The cases referred to scrutiny in the United Kingdom by the Secretary of State in respect of warrants for interception issued under the Regulation of Investigatory Powers Act 2000. In the United States, the Privacy and Civil Liberties Oversight Board is required to continually review the regulations and information-sharing practices of the intelligence services.[697] Claims have been made, both successfully and unsuccessfully, that the United States intelligence services have exceeded their authority when collecting telephone records, such as in the cases of *American Civil Liberties Union v Clapper* and *Klayman v Obama*.[698] In response to concerns about transparency and the potential for human rights violations, the Privacy and Civil Liberties Oversight Board has recommended changes specifically to the treatment of telephone records and more generally to the collection of information from other companies and foreign governments.[699]

---

[694] For example, see Melanie Newman "Pressure on GCHQ to Disclose Internal Policies After Historic Tribunal Ruling" (6 February 2015) The Bureau of Investigative Journalism <www.thebureauinvestigates.com>; Liat Clark "Five Eyes Intelligence Pact to be Scrutinised by European Court" (9 September 2014) Wired <www.wired.co.uk>; Ian MacLeod "Spy Versus Spy: Australian Security Oversight Holds Lessons for Canada" *The Ottawa Citizen* (online edition, Ottawa, 18 March 2015) and Conor Friedersdorf "Is 'The Five Eyes Alliance' Conspiring to Spy on You?" (25 June 2013) The Atlantic Monthly Group <www.theatlantic.com>.

[695] *Belhadj v the Security Service, SIS, GCHQ, Home Office and FCO* [2015] IPT/13/132-9/H, *Liberty (The National Council of Civil Liberties) and Others v the Secretary of State for Foreign and Commonwealth Affairs and Others* [2015] IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH.

[696] Investigatory Powers Tribunal "Investigatory Powers Tribunal Report: 2011-2015" (2016) Investigatory Powers Tribunal <ipt-uk.com>, at 26 and 27.

[697] 118 Stat 3638 Intelligence Reform and Terrorism Prevention Act 2004 (United States), s 1061.

[698] *American Civil Liberties Union v Clapper* 785 F 3d 787 (2d Cir 2015) and *Klayman v Obama* 957 F Supp 2d 1 (DC Cir 2015).

[699] "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court" (2014) Privacy and Civil Liberties Oversight Board <www.pclob.gov>, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (2014) Privacy and Civil Liberties Oversight Board <www.pclob.gov>, at 134-137 and 145–147, and "Recommendations Assessment Report" (2015) Privacy and Civil Liberties Oversight Board <www.pclob.gov>, at 3,4 and 12–14.

In New Zealand, scrutiny is provided by the Inspector-General and Deputy Inspector-General of Intelligence and Security who inquire into the activities of the intelligence and security agencies and investigate complaints.[700] The issue of surveillance warrants is authorised by a Commissioner of Intelligence Warrants and an authorising Minister.[701] The Commissioner of Warrants must previously held office as a Judge of the High Court.[702] In Canada there is judicial control of the issue of interception warrants and oversight of activities is provided by the Security Intelligence Review Committee.[703] In Australia the Inspector-General of Intelligence and Security provides the same oversight.[704] Nonetheless, that oversight occurs in secrecy and the criteria against which invasions of privacy are authorised remains secret. In that respect, the European Court of Human Rights said in *Bykov v Russia*:[705]

> Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive – or to a judge – to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

The secrecy surrounding the Five Eyes agreement means its terms cannot be analysed in detail. Moreover, the details of the agreement that have been declassified show that the arrangement is focussed on sharing the product of intercepted foreign communications and not information from other sources of intelligence. For that reason, it is suggested that the Five Eyes agreement is not a suitable vehicle for intelligence-sharing via a single window.

### *B The INTERPOL System 1956*

The rules of the INTERPOL system are unsuitable to use for sharing intelligence through a single window system.[706] The purpose of the INTERPOL system is to support different needs, not customs matters. Information must be held in a central database accessible by all member states. The 1996 Europol system for European policing cooperation also uses a

[700] Intelligence and Security Act 2017 (New Zealand), ss 156-158.

[701] Section 62.

[702] Section 113.

[703] Canadian Security Intelligence Service Act 1985 (Canada SIS Act) (Canada), ss 21 and 34.

[704] Inspector-General of Intelligence and Security Act 1986 (Australia).

[705] *Bykov v Russia* (4378/02) Grand Chamber, ECHR 10 March 2009, at [78].

[706] See INTERPOL "Rules on the Control of Information and Access to INTERPOL's Files II.E/RCIA/GA/2004(2009)" (2009) INTERPOL <www.interpol.int> and INTERPOL "INTERPOL's Rules on the Processing of Data III/IRPD/GA/2011(2016)" INTERPOL (2016) <www.interpol.int>.

central database.[707] This creates a risk that information will be used for purposes for which it was not originally supplied. The supplier of information to the INTERPOL system loses the ability to control the access to and use of that information. There can be no confidence that information will be removed from the database when it is no longer required and this increases the risk of unauthorised disclosure. The rules allow any person to access all information held about themselves, which satisfies the Privacy Principles, but would enable secret intelligence to be disclosed if it was held in the system.

INTERPOL began in 1914 as the International Criminal Police Congress (ICPC) at Monaco.[708] In 1949 the United Nations granted the organisation consultative status as a non-governmental organisation.[709] In 1956 it changed its name to INTERPOL.[710] It now has 190 member states.[711]

The aims of the INTERPOL arrangement are:[712]

1. To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the "Universal Declaration of Human Rights";
2. To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes.

Paragraph 2 above indicates general support for the law enforcement activities of customs authorities. On the other hand, the use of INTERPOL information is restricted to "the purposes of international police cooperation".[713] The constitution of INTERPOL established a Commission for the Control of Files to ensure the processing of personal information complies with INTERPOL's own rules.[714]

INTERPOL's rules include the creation of databases of information submitted by member states.[715] Information in the INTERPOL databases may be accessed by all member states of

[707] Regulation 2016/794, above n 20, arts 17, 18 and 20.

[708] INTERPOL "History" (2015) INTERPOL <www.interpol.int>.

[709] Ibid.

[710] Ibid.

[711] INTERPOL "Overview" INTERPOL (2015) <www.interpol.int>.

[712] INTERPOL "Constitution of the ICPO-INTERPOL I/CONS/GA/1956(2008)" INTERPOL (2008) <www.interpol.int>, art 2.

[713] INTERPOL "INTERPOL's Rules on the Processing of Data III/IRPD/GA/2011(2016)" INTERPOL (2016) <www.interpol.int>, art 56(1) (b).

[714] INTERPOL, above n 712, art 36.

[715] INTERPOL, above n 713, arts 29–72.

INTERPOL.[716] This is not ideal as states may wish to share information with individual states or a small group of states. When supplying information to the INTERPOL databases, member states can record additional access restrictions for that information.[717] Because the purpose of the INTERPOL system as stated above is "widest possible mutual assistance", it seems unlikely that recording an access restriction to allow retrieval by only one other state or a small group of states would be acceptable.

Mandatory minimum requirements for information submitted to INTERPOL databases include:[718]

(a) the identity of the source of the data;
(b) the date on which the data were recorded;
(c) the specific purpose for the recording;
(d) for any personal data, the status of the person and the data connecting this person to an event;
(e) the level of confidentiality of the data;
(f) the initial retention period of the data;
(g) access restrictions;
(h) any additional information ensuring that all the data are relevant to the purpose and of interest for the purposes of international police cooperation.

These conditions meet some of the requirements of the Privacy Principles. States must ensure that the information they access in INTERPOL databases is accurate before it is used.[719] They must do this by directly contacting the state that supplied the information to the database. This requires every member state to have effective relationships in place with other member states for this purpose. The member states that supply information also have an obligation to keep the information up to date.[720]

INTERPOL's rules state that any person may access any personal information held about that person which has been recorded by INTERPOL, free of charge.[721] It does not appear that there are any rules that enable INTERPOL to withhold intelligence information from that person which might be deemed a secret by the supplying member state.[722] There are

[716] Article 54(1).

[717] Article 37.

[718] Ibid.

[719] Article 63.

[720] Article 46.

[721] INTERPOL, above n 706, art 9 (a).

[722] Ibid.

confidentiality rules for information on the INTERPOL databases, but these do not prevent any information about a person being disclosed to that person.[723]

Member states may submit information to INTERPOL's databases with a request to publish a notice classified by colour. Red notices provide information for the purpose of locating and arresting a wanted person so they may be extradited.[724] Green notices are published to warn about a person's criminal activities.[725] Blue notices seek additional information about a person to assist with an investigation.[726] Yellow notices are issued to locate a missing person or identify a person unable to identify himself or herself.[727] Black notices are published to identify dead bodies. Purple notices are issued to warn about methods used in the committing of an offence and to seek information to aid an investigation.[728] Orange notices warn about an event, a person, an object or a method of offending that represents an imminent threat to public safety.[729] There are also notices that have no colour code, which are used to locate stolen works of art or important cultural artefacts, or provide information about a person or an entity that is subject to UN Security Council sanctions.[730]

The collection of information and the entry of that information into INTERPOL system must be lawful and in accordance with the Universal Declaration of Human Rights.[731] In this respect, the INTERPOL system is superior to all the other agreements evaluated here.

Real-time information exchange is possible through system interconnections that satisfy INTERPOL requirements, but the system is not designed for this.[732]

Information-sharing with INTERPOL is enabled in New Zealand by the Mutual Assistance in Criminal Matters Act 1992 and principle 10 of the Privacy Act 1993 which allows personal information to be used for law enforcement and public safety purposes.[733] The Privacy Act 1993 also allows the overseas transfer of personal information that is "required by any Convention or other instrument imposing international obligations on New

[723] INTERPOL, above n 713, art 112.

[724] Article 82.

[725] Article 89.

[726] Article 88.

[727] Article 90.

[728] Article 91.

[729] Article 93.

[730] Articles 94 and 95.

[731] Article 11.

[732] Article 55.

[733] Section 6, principle 10 ss (c) and (d).

Zealand".[734] There is also a general exemption to principles 1 to 5 and principles 8 to 11 of the Act for the GCSB and the NZSIS.[735] Principles 6 and 7 provide individuals with the ability to access and correct their personal information. The Act enables the NZSIS and GCSB to keep the existence of intelligence secret, which frustrates the application of these two principles.[736] Similarly, the OIA enables government agencies to refuse an individual access to personal information if disclosing that information would prejudice maintenance of the law, national security or the safety of any person.[737] The Act also enables government agencies to deny the existence of information.[738] Individuals may lodge a complaint with the Office of the Ombudsman if they have been refused access to their personal information, or the existence of the individual's personal information has been denied, or their personal information has been mishandled by a law enforcement or security agency.[739] If the Office of the Ombudsman chooses to investigate the complaint, it will consult with the Inspector-General of Security on matters within the jurisdiction of the Inspector-General.[740]

The purpose of the system is inclined towards policing matters and not customs matters. Also, the rules require information to be held in a central database accessible by all member states. Holding information in a centralised database creates a risk that information will be accessed and used for purposes for which it was not originally supplied. The state party that supplies information to the INTERPOL system loses the ability to control the access to and use of that information. Careful management is needed to ensure information is deleted from the database when it is no longer required. Otherwise, the presence of information in the database for extended periods increases the opportunity for unauthorised disclosure. Furthermore, the rules allow any person to access all information held about them and while this satisfies the Privacy Principles, it could result in the unwanted disclosure of secret intelligence. The INTERPOL rules also state the particular types of information to be shared, but do not set out standards for the format of data.

Thus, the INTERPOL system is not ideal for intelligence-sharing via a single window system.

[734] Section 114B(3)(b).

[735] Section 57.

[736] Section 32.

[737] Section 27.

[738] Section 10.

[739] Ombudsmen Act 1975 (New Zealand), s 13.

[740] Sections 17C and 21C.

### *C PNRGOV System 2013*

In 2013, a collaboration between the WCO, IATA and ICAO produced updated standards for Passenger Name Record (PNR) and Advance Passenger Information (API).[741] This system is called PNRGOV.

The system allows government border agencies and airlines to confirm that a passenger has the appropriate documentation for departure from a state and authority to enter the destination state, such as passport and an entry visa.[742] The documentation states that airlines should take into account national privacy laws "on a case-by-case basis" and there are no specific rules implementing the Privacy Principles.[743] The PNRGOV system is used by government agencies to risk-manage passengers and their baggage. The system contains personal information, but it is not used for sharing secret intelligence information. This is because information is stored in the databases of both the airlines and the government authorities that receive the information. Consequently, an arrangement like the PNRGOV is unsuitable for the purposes of the proposed legal framework.

PNRGOV is overseen by the WCO, IATA and ICAO. IATA is a trade association of the world's airlines. ICAO is the international body representing the airspace regulators that codify rules for air navigation and the use of airspace. In this triumvirate, the WCO represents the interests and requirements of the government border agencies that seek to use the information. ICAO, representing the various national regulators, can implement rules that require carriers to provide this information in a particular format. IATA oversees the implementation of the rules by its member organisations – the air transport operators.[744] API is extracted from an IATA member database. API guidelines include data formatting standards for various information including name, gender, date of birth, nationality and visa details.[745]

Border agencies and airlines use this information before and at check-in to confirm that a passenger has the appropriate documentation for departure from a state – usually a valid

---

[741] WCO "ICAO, WCO and IATA Guidelines on Advance Passenger Information (API)", above n 674.

[742] At 9–12. See Julian Grenfell and Richard P Wright *The EU/US Passenger Name Record (PNR) Agreement: Report with Evidence, 21st Report of Session 2006-07* (Her Majesty's Stationery Office, London, 2007); Els De Busser *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities* (Maklu, Antwerp, 2009), at 359 and Ruwantissa Abeyratne *Strategic Issues in Air Transport: Legal, Economic and Technical Aspects* (Springer Science and Business Media, Montreal, 2012), at 219.

[743] WCO, above n 674, at 25.

[744] Some of the experts that were interviewed indicated that a collaboration like this between international bodies might be an alternative way to implement the proposed legal framework. Their views on implementation are discussed further in Chapter Seven.

[745] WCO, above n 674, at 20.

passport – and authority to enter the destination state, such as an entry visa.[746] Specifically:[747]

> Advance Passenger Information (API) involves the capture of a passenger's biographic data and other flight details by the carrier prior to departure and the transmission of the details by electronic means to the Border Control Agencies in the destination country. API can also act as a decision-making tool that Border Control Agencies can employ before a passenger is permitted to board an aircraft. Once passengers are cleared for boarding, details are then sent to the Border Control Agencies for screening against additional databases and can identify passengers and crew of interest including those subject to United Nations Security Council sanctions lists and travel bans. While this technique is beginning to be used by more and more Border Control Agencies it has been used by a number of countries for some time. API has the potential to considerably reduce inconvenience and delays experienced by passengers as a result of necessary border processing. It also provides a system which carriers can use to comply with relevant legislation of the countries they fly to including legislation implementing travel bans against those on United Nations Security Council sanctions lists.

The PNR data is also an extract from an IATA member database. It contains standardised information about a passenger's travel booking such as the date of ticket issue, the date of intended travel, seat number, the travel itinerary for the specific passenger and the names of other passengers on the travel record.[748]

The PNR and API documentation produced by WCO, IATA and ICAO recognises that different privacy law exists in each state.[749] The documentation declares that each airline should consider the privacy laws of the state with which they are exchanging information "on a case-by-case basis".[750] The EU has made agreements with Australia, Canada and the United States for the transfer of PNR data.[751]

---

[746] Ibid, at 9–12. See also Grenfell and Wright, above n 742 and Abeyratne, above n 742.

[747] WCO, above n 741, at 8.

[748] WCO "ICAO, WCO and IATA Principles, Functional and Business Requirements: PNRGOV" (October 2013) WCO <www.wcoomd.org> and WCO "ICAO, WCO and IATA Management Summary on Passenger Related Information" (2013) WCO <www.wcoomd.org>, at 2.

[749] WCO, above n 741, at 25.

[750] Ibid.

[751] Agreement between the European Union and Australia on the Processing and Transfer of Passenger Name Record (PNR) Data OJ L186/4 (2012); Agreement between the European Community and the Government of Canada on the Processing of Advance Passenger Information and Passenger Name Record Data OJ L82/15 (2006) and Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records OJ L215/5 (2012).

The EU has recognised the adequacy of New Zealand privacy law for this and other kinds of information exchange, by deciding:[752]

> For the purposes of Article 25(2) of Directive 95/46/EC, New Zealand is considered as ensuring an adequate level of protection for personal data transferred from the Union.

The EU had a similar arrangement in place with the United States in the form of Commission "safe harbour" Decision 2000/520/EC.[753]

In New Zealand, the authority to use PNR and API information is contained within the Customs and Excise Act 1996 and the Immigration Act 2009.[754]

Air transport operators have an incentive to ensure each passenger is authorised to enter the country of destination. If New Zealand is the country of destination, that incentive is the avoidance of costs associated with holding that person in detention, returning that passenger to their country of origin and the avoidance of fines payable under New Zealand law.[755]

There is no explicit reference to lawful collection in the PNR and API documentation. All information in the PNR and API record is collected from the passenger by the air transport operator and its agents.

On 6 October 2015, the European Court of Justice ruled in *Schrems v Data Protection Commissioner* that Commission Decision 2000/520/EC is invalid.[756] This judgment overturned the Commission's determination that "safe harbour" privacy principles issued by the United States Department of Commerce were adequate for compliance with EU privacy law. It also contradicted a 2013 report from the European Commission that stated that the United States Department of Homeland Security was "operating in compliance with the standards and representations in the agreement with the EU".[757]

---

[752] Decision on the Adequate Protection of Personal Data by New Zealand [2013] OJ L28/12, art 1.

[753] Decision 2000/520/EC: Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions issued by the US Department of Commerce [2000] OJ L215/7.

[754] Customs and Excise Act 1996 (New Zealand), s 38E and Immigration Act 2009 (New Zealand), ss 96, 101 and 102.

[755] Immigration Act 1987 (New Zealand), s 96; Immigration (Carriers' Infringement Offences, Fees and Forms) Regulations 2012 SR 2012/106 (New Zealand), schedule 1 and Immigration New Zealand "People Travelling to New Zealand: Information for Airlines" (August 2014) Immigration New Zealand <www.immigration.govt.nz>, at 2.

[756] C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECR I-650.

[757] Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Records to the United States Department of Homeland Security

A report issued 3 months before the *Schrems* judgment by the Privacy Office of the United States Department of Homeland Security had also stated that its use of PNR data was compliant with the privacy controls of the agreement with the EU.[758]

The *Schrems* judgment found that there were inadequate protections against information disclosure to the United States government without the knowledge and consent of the information subject.[759] The *Schrems* judgment cast doubt on the information-sharing agreements made under the "safe harbour" provisions. The data protection authorities of EU member states can now examine each and every privacy sharing arrangement and make their own determinations of privacy adequacy.

In 2016 a directive was issued by the European Parliament regarding the exchange of PNR information with other states.[760] The directive requires member states to ensure data is "transferred to a single designated [collection point] in the relevant member state".[761] Member states must "take all necessary measures to enable air carriers to fulfil their obligations under this Directive".[762] In July 2017, the European Court of Justice issued an opinion on a proposed agreement for sharing PNR data between the EU and Canada.[763] The opinion stated that the proposed agreement was incompatible with EU privacy law.[764] It included 7 conditions that must be met for the agreement to be compliant with EU law, including: guaranteed independent oversight; restrictions on the sharing of information with a 3rd state; and limiting the use of PNR information to the fight against terrorism and serious transnational crime.[765]

It is important to note that the PNR and API information is extracted from databases owned by the airline companies. State authorities use this information for risk-management purposes, but cannot make changes to this information for reasons such as personal information being inaccurate.

---

[2013] COM(2013) 844, at 2, and OJ L215/5 (2012), above n 751. Note that the European Commission report also recommended some issues that needed to be addressed.

[758] "A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States" (2015) United States Department of Homeland Security <www.dhs.gov>, at 11–29.

[759] *Maximillian Schrems v Data Protection Commissioner*, above n 756, at [87] – [89].

[760] Directive 2016/681/EU on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132.

[761] Ibid, at [13].

[762] Ibid, at [18].

[763] Opinion 1/15 of the Court (Grand Chamber) [2017] ECR 592.

[764] Ibid, at para 232(2).

[765] Ibid, at para 232(3).

The PNRGOV system is used to provide state authorities with information useful for the risk-management of passengers and their baggage. Although it is a system that contains personal information, it is not a system used for sharing secret intelligence information. Information is not stored centrally, rather it is stored in the databases of the individual airlines and the government authorities that also receive the information. Consequently, the terms for this arrangement are not suitable for multilateral intelligence-sharing through a single window system.

### *D Summary of Multilateral Agreements*

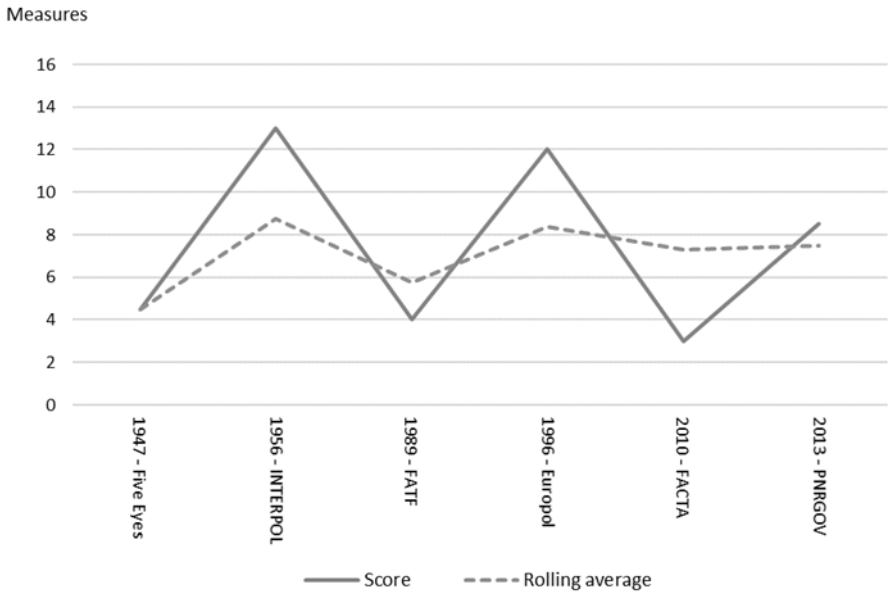
The assessment of other models for information-sharing against the measures established in Part I is summarised in Table 10.

**Table 10. Summary of other information-sharing model assessments**

| *Theme* | Requirement | 1947 – Five Eyes | 1956 – INTERPOL | 1989 – Financial Action Task Force | 1996 – Europol | 2010 – Foreign Account Tax Compliance Act | 2013 – PNRGOV |
|---|---|---|---|---|---|---|---|
| | | (✓) Meets, (P) Partially meets, or (×) Fails to meet | | | | | |
| *Trust between states that intelligence is secured, accessed and used appropriately* | Information access and disclosure control | P | P | × | ✓ | × | ✓ |
| | Audit, review or self-reporting of compliance | × | × | × | P | × | × |
| | Information retention and destruction controls | × | ✓ | × | ✓ | × | × |
| | Information is held by each state, rather than stored in a single, central database (Big Data) | ✓ | × | ✓ | × | ✓ | × |
| *State autonomy* | Voluntary, not compulsory, information-sharing | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| *Include the Privacy Principles* | Collection Limitation | × | P | × | P | × | P |
| | Data Quality | × | ✓ | × | ✓ | × | P |
| | Purpose Specification | × | ✓ | × | ✓ | × | P |
| | Use Limitation | × | ✓ | × | ✓ | × | P |
| | Security Safeguards | × | ✓ | × | ✓ | × | P |
| | Openness | × | ✓ | × | ✓ | × | P |
| | Individual Participation | × | ✓ | × | ✓ | × | P |
| | Accountability | × | ✓ | × | ✓ | × | P |
| *Promote access to justice, prohibit information gained through arbitrary search and seizure and prohibit information gained through torture* | Information is collected lawfully | × | ✓ | ✓ | × | × | ✓ |
| *Implement intelligence-sharing through a single window* | Enables intelligence-sharing | ✓ | P | ✓ | ✓ | ✓ | P |
| | Common standards/ format for information and processing | × | P | × | × | × | ✓ |
| | Enables real-time electronic exchange | ✓ | ✓ | × | ✓ | × | ✓ |

Figure 13 illustrates the extent to which each of these models have implemented the measures identified in Part I.

**Figure 13. Implementation of the measures in other models for information-sharing**




The graph in Figure 13 shows a slight rise over time in the average number of measures that were implemented in the models examined here, although the small sample size makes this trend inconclusive. A clearer trend is evident in the graph at the end of this Chapter that compares these agreements with the bilateral and multilateral agreements that were examined.

The 1956 agreement for the INTERPOL system had evolved over time and it implemented 14 of the 16 measures. The agreements involving the EU generally implemented more of the measures than the other agreements

## *V Chapter Summary*

This demonstrated that there is no existing law that would enable customs administrations to share intelligence through a single window system. A set of measures was used to compare the agreements with the operational and human rights requirements that had been identified in previous Chapters.

The analysis in this Chapter revealed how agreements have evolved alongside the development of electronic information systems.

The early agreements assessed against these measures, like the Five Eyes agreement, pre-dated the development of computer technology. The first agreement to enable the real-time electronic exchange of information was in 1996.[766] Not all subsequent agreements provided for this capability.

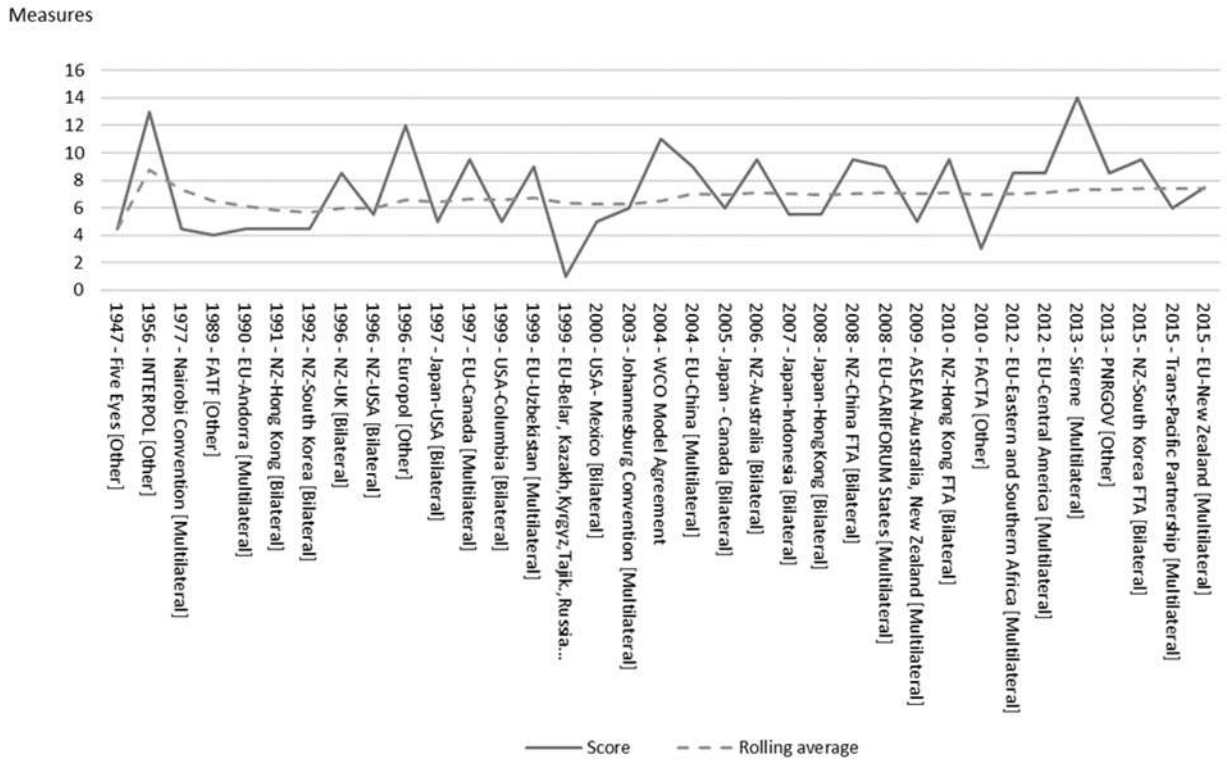
[766] 1996 New Zealand – United Kingdom Agreement, above n 94.

Of all the agreements and models that were evaluated, the SIRENE system has terms most suitable for replication for intelligence-sharing via a single window system. Even so, the SIRENE system and the INTERPOL system both require the submission of information to a central database that is accessible by the authorities of all member states. The SIRENE and INTERPOL systems are suitable for the purposes for which they were designed, but the central databases they use are undesirable for intelligence-sharing as the reduces the secrecy of the information they contain.

An ideal system would combine publicly available information about what information is being exchanged and for what purpose, like the PNRGOV system, with well understood and accepted rules for accessing processing and managing personal information, like the SIRENE system.

**Figure 14** shows the extent to which each of the agreements that were examined satisfy the measures established in Part I. The graph in **Figure 14** shows that there has been a small rise over time towards implementing the measures identified in Part I.

Figure 14. Comparison of all models to the measures established for the legal framework




Chapter Six presents the legal framework that was developed to satisfy the measures established in Part I and to enable customs to share intelligence through a single window system.

# Chapter Six – Outline of the Proposed Legal Framework

This Chapter introduces a legal framework for intelligence-sharing through the single window that includes transparent protection for human rights. It is the product of the reasoning in the previous Chapters. It combines the needs of customs administrations for intelligence-sharing that were discussed in Chapter Two with evident protection of the privacy and other human rights that were discussed in Chapter Three and Chapter Four. It makes the terms for managing information explicit, even though the information and the ways in which it is used must remain secret.

The legal framework presented here comprises a draft international Convention for intelligence-sharing and a Model Law for domestic implementation. They are included respectively in Appendix Two and Appendix Three

References to the articles in the proposed Convention are identified as art or arts and references to sections in the Model Law are labelled s or ss.

This Chapter is made up of three Parts.

Part I describes the articles of the proposed Convention and the sections of the Model Law that set out the purpose of the legal framework.

Part II describes the intelligence sharing process. It shows how the proposed legal framework implements the process. It also shows how the measures listed in Chapter Five are pragmatically satisfied.

Part III summarises this Chapter.

## *I The Purpose of the Legal Framework*

The preamble establishes the overarching goals of the Convention which is to enable intelligence-sharing for customs' purposes with clear terms to protect human rights. It refers to international agreements and aspirations for improving trade facilitation through shared information for customs risk-management. It also refers to the international aspirations and obligations for human rights protection recorded in the United Nation's Charter and the ICCPR. The purpose is stated explicitly in art 1 with text that is mirrored in s 3 as follows:

> …for the purposes of applying, investigating, or prosecuting breaches of customs law, for risk-management and for the prevention of customs offences.

Article 1 also states that intelligence-sharing is voluntary under the agreement. This is reflected in s 5(6) which states:

> Any intelligence-sharing carried out under this Act is voluntary and [Insert Customs Agency] may not compel another customs administration to provide intelligence related to any trade transaction.

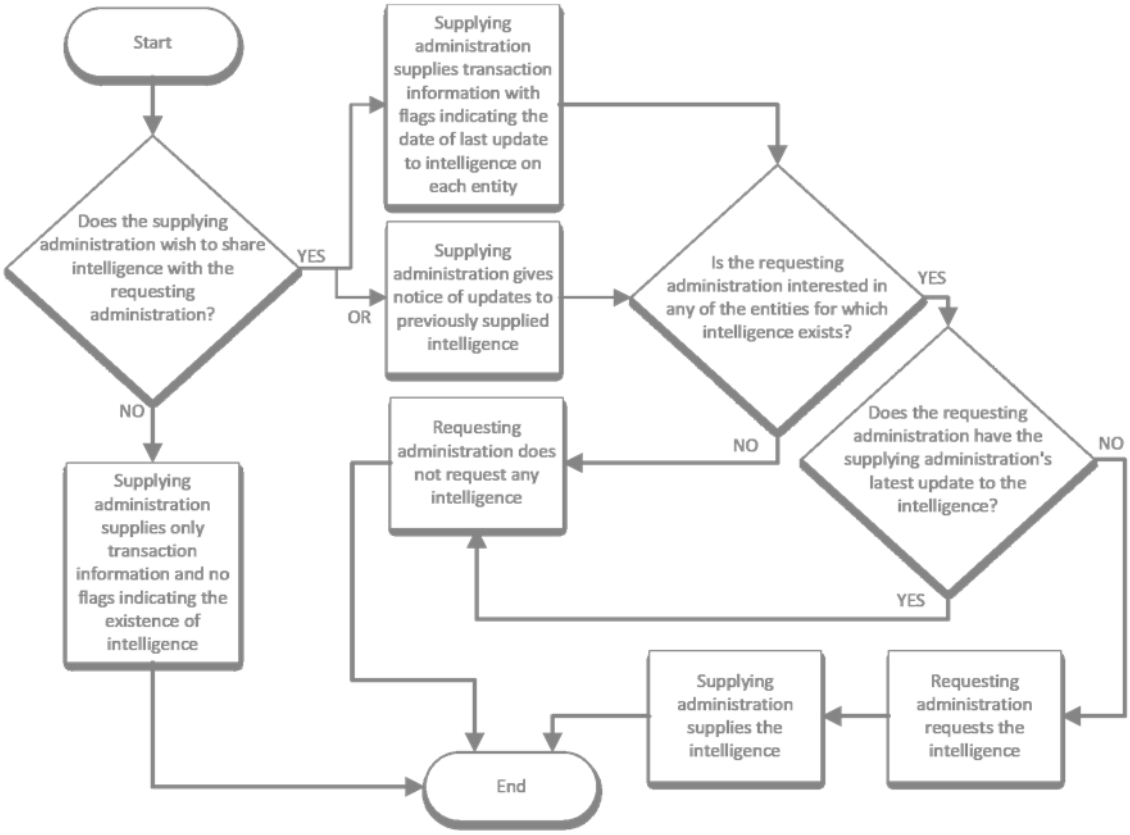
Article 7 and s 5(7) restrict the use of information to the purposes set out in the Convention and the Model Law. These articles and sections help to implement in particular the Privacy Principles of Purpose Specification and Use Limitation.[767]

Article 2 and s 6 set out the types of information which may be shared, using broad definitions to cover any information that may be relevant to customs risk-management. Article 3 and s 6 have an additional stipulation that the information is to adhere to formats and standards published by the WCO from time to time.

## *II The Intelligence-sharing Process*

The intelligence-sharing process is established in art 3 and ss 7 and 11. The diagram below illustrates the process. The diagram also shows how updates can be made to information, independent of any transaction. Updating information is stipulated in arts 10 and 11 and s 10.

**Figure 15. The proposed single window intelligence-sharing process**




[767] The Privacy Principles of Purpose Specification and Use Limitation are described in Chapter Four.

The process relies on information flags associated with each entity involved in a transaction. The information flags reveal the date on which the intelligence which may be shared was last updated. The requesting administration can request the information or any updates it has not previously received.

The process is described in art 3 below.

Information-sharing process

Article 3

1. Providing administrations may share specific information in advance of the departure of goods from their territories.

2. To reduce duplication in information-sharing, the following procedures will apply –

   (1) The providing administration may include with the information related to any trade transaction a declaration that intelligence exists which may be shared;

   (2) The requesting administration may request all the intelligence that may be shared if –

      (a) the requesting administration has not previously been provided with the intelligence holding; or

      (b) the intelligence has been previously provided and has been destroyed under article 10.

   (3) The providing administration shall provide information that specifies the date that an update was last made to the intelligence that may be shared.

   (4) The requesting administration may request the update to the intelligence if that update has not previously been received.

   (5) The providing administration shall provide the intelligence or the update as requested by the requesting administration.

3. All requests, notices and other information shared under this Convention shall be transmitted electronically using standards for data type and format published by the World Customs Organisation for this purpose.

*A Reservations and Non-Compliance*

Before sharing information, art 4 and s 9 require a customs administration to consider the reservations to the Convention made by the requesting administration. This requirement reinforces the voluntary nature of intelligence-sharing and it provides further opportunity to withhold intelligence. Article 8 and ss 8 and 9 also require a customs administration to

refrain from sharing information if it becomes aware that the requesting customs administration is or will be non-compliant with the terms of the Convention. These terms enable the providing administration to apply diplomatic pressure on the requesting administration to conform to the purposes of the Convention, by informing it that intelligence exists but it will not be shared.

To avoid applying that diplomatic pressure, a providing administration could simply withhold the information flags that reveal it has intelligence that may be shared. As a result, the requesting administration would not be aware that the intelligence existed and had not been provided.

### *B Avoiding Manipulation*

Article 5 and s 7 prevent State Parties from sharing untruthful information aimed at manipulating trade. Article 5 states:

Untrue Information

Article 5

1. No state party shall share information that it knows or suspects to be untrue without also sharing a statement of that suspicion.
2. No state party shall share information that it knows or suspects to be untrue for the purpose of interfering with the legitimate trade of another state party.
3. State Parties shall take reasonable steps to validate provided information to ensure legitimate trade is not inhibited by information that is known or suspected to be untrue.

### *C Lawfully Obtained Information*

This legal framework aims to implement a process for sharing information, not collecting information. Nevertheless, it also aims to include transparent protection against torture and arbitrary search and seizure. To this end, art 7 and s 7 compel customs administrations to disclose or accept only information that was obtained by lawful means.

### *D Available Process to Challenge the Accuracy of Information*

Shared information can be used in judicial processes under art 6 and s 8. This article and section ensure that individuals are able to challenge and defend themselves against the information used in judicial processes, which is a requirement of the principle of Individual Participation. These inclusions help to implement the Individual Participation principle.

### *E Maintaining Confidentiality*

Article 8 and s 8 stipulate that access to and the use of information must be strictly controlled. This text supports the Security Safeguards and Purpose Specification principles. It requires a requesting administration to implement any specific security

requirements imposed by a supplying administration. Article 8(12) and s 7(6) also place an obligation on customs administrations to notify requesting administrations of security breaches.

Confidentiality

Article 8

1. Information shared under this Convention shall be treated as confidential by the customs administrations of the territories from which the goods will depart, through which transshipment occurs and in which the goods will arrive.

2. Any intelligence shared under this Convention shall be used only by the officials of the requesting state party and shall not be disclosed to any other state party, customs administration, organisation or person except with the express permission of the providing administration.

3. The requesting administration shall limit access to the provided information to officials for the purposes specified in paragraph 1 of article 1.

4. The requesting administration shall protect provided information to prevent unauthorised disclosure.

5. The requesting administration shall adopt such additional conditions for access to, use of, storage, transmission, correction and destruction of intelligence as may be required by the providing administration.

6. A providing administration shall not impose unreasonable or unnecessary conditions for access to, use of, storage and transmission of information.

7. The requesting administration shall disclose to the providing administration a summary of the protection afforded to the provided information on the first occasion information is provided and at least annually thereafter.

8. The requesting administration may use intelligence provided under this Convention as evidence in a prosecution or in support of any other judicial process.

9. To enable compliance reviews or audits the requesting administration shall record each access to the provided information and that record shall contain the date and time the information was accessed, the details of the person or persons accessing the information and the reason or purpose for accessing the information.

10. The providing administration shall ensure the transmission of information to a requesting administration is secured against unauthorised disclosure.

11. The providing administration shall refrain from providing information including intelligence to a requesting administration if the requesting administration fails to observe the terms of this Convention.

12. The requesting administration shall give notice of any unauthorised disclosure of information and the steps that have been or will be taken to remedy that situation to the providing administration and wherever possible to the subject of the information if that subject is likely to be adversely affected.

Article 8 and s 11 require that the access to and use of information shared under the legal framework is recorded for audit purposes. This audit record helps to implement the Accountability principle by ensuring customs administrations are accountable for the security and use of the information they receive. It also supports the role of the data controller by providing evidence of a customs administration's compliance with the terms of the Convention.

Paragraph 8 of art 8 appears to conflict with the notion that intelligence is information that must be kept secret. This paragraph and corresponding text in s 8(13) enable intelligence to be used as evidence in a prosecution or in support of other judicial processes such as the issuing of search warrants. These clauses recognise that disclosure of intelligence can be compelled by a court order and no foreign agency can countermand or impose conditions on access to information ordered to be produced by a domestic court.

### *F Transshipments*

Trade logistics sometimes require traded goods to travel through the territory of a third-party state. This is called a transshipment. Article 9 and s 7 enable the sharing of information with a third-party state to enable its risk-management of that transshipment.

### *G Correcting and Updating Information*

A supplying administration is required by arts 10 and 11 and s 10 to periodically review intelligence and provide updates or corrections to a requesting administration.

Intelligence can be updated or corrected without a trade transaction taking place at the same time. In this way, a requesting administration will always use the most accurate and complete information in its risk-management processes, thereby supporting the Data Quality principle.

Article 10 and s 10 require information to be periodically reviewed and destroyed if it is no longer required.

Correction, retention and destruction of information

Article 10

1. The requesting administration may indefinitely retain any personal information it has been provided if that information is essential for –

   (1) a criminal investigation or prosecution;

   (2) the risk-management of on-going trade transactions; or

   (3) the maintenance of accurate and complete records of decisions.

2. The requesting administration shall destroy any personal information included in provided information within six months of that information being received if the information is not essential for a purpose described in paragraph 1 of this article.

3. The requesting administration shall review the provided information every six months and destroy any personal information that is no longer deemed essential.

4. A providing administration may at any time require the correction of information it has provided to the requesting administration, and –

   (1) upon receipt of such a request, the requesting administration shall without delay record the correction to the information it has been provided; or

   (2) if the requesting administration must maintain an original record of the information that was provided, it shall record a reference to the correction it has received as an addendum to the original record.

5. The providing administration may at any time require the destruction of intelligence it has provided to the requesting administration.

6. Upon receipt of a request from a providing administration to destroy intelligence that it has provided, the requesting administration shall without delay destroy all records of that intelligence.

7. State Parties shall ensure that every organisation or person has access to a process by which they may view and correct any information other than intelligence about themselves which is shared under this Convention.

These clauses support the Collection Limitation and Use Limitation principles by ensuring that information which is no longer required is no longer stored. They support the Data Quality principle by ensuring that stale and potentially inaccurate information is not retained. They also support the Security Safeguards principle because information which is no longer retained cannot be inappropriately disclosed.

### *H Notice to Subjects of Information*

Although the legal framework implements a process for sharing information and not collecting information, art 12 and ss 5 and 12 require the knowledge and consent of the subject of information at the time of collection. Consent is mandatory unless the existence of the information must be kept secret from the subject. This text helps to implement the Collection Limitation and Openness principles as much as is practical in an intelligence-sharing context.

Reasons for not obtaining the knowledge and consent of the data subject are set out in art 12 as follows.

Notice to the subjects of information

Article 12

1. State Parties shall inform the subjects of the information at the time it is collected that the information may be shared under this Convention, except where informing the subject is not possible or for compelling reasons of public good.
2. For the purposes of paragraph 1 of this article, compelling reasons of public good are –
   (1) that informing the subject will impede the effective application, or investigation or prosecution of a breach of customs law; or
   (2) that informing the subject will reveal aspects of the risk-management process that would enable the subject or others to take steps in future to defeat the risk-management process.

### *I The Data Controller*

The data controller is a central point through which the subjects of information can access and correct information held about themselves. In cases where information must be kept secret from the information subject, the data controller advocates for their privacy rights through compliance audits. This role supports the principle of Accountability by ensuring someone within the customs administration is accessible and accountable for the way the organisation handles personal information. However, the creation of the role within the customs administration creates a risk of conflict of interest. In New Zealand, this risk is balanced by the complementary roles of the Privacy Commissioner and Ombudsmen which are roles outside the customs administration that hold the organisation to account, while the data controller is a role within the organisation that is accountable for the control of personal information.[768] The data controller is similar to the organisational Chief Privacy Officer recommended to businesses by the Japanese government.[769]

[768] The functions of these external roles are described at Privacy Act 1993 (New Zealand), s 13 and Ombudsmen Act 1975 (New Zealand), s 13.

[769] Ministry of Economy, Trade and Industry (Japan), above n 489, at 33.

Balancing that risk is the benefit that a data controller within the customs administration will have easier access to customs people, information and processes than if the role was external to the organisation.

The role of the data controller is established in art 13 and s 13. The role is described as follows.

Data Controller

Article 13

1. Each state party shall appoint an official of its customs administration as a data controller to be accountable for compliance with the terms of this Convention.

2. The data controller shall have the authority to conduct compliance audits of the information processing systems of the customs administration periodically at his or her discretion.

3. Any organisation or person shall have the right to request from the data controller confirmation of whether or not the customs administration has information relating to that organisation or person.

4. Any organisation or person shall have the right to request and be provided any data related to that organisation or person –

   (1) within a reasonable time;

   (2) at a cost that does not exceed the actual cost of researching and collating the information; and

   (3) in a form that can be reasonably expected to be understood by that organisation or person.

5. Any person may challenge the accuracy of the information relating to that person and –

   (1) have that information corrected;

   (2) have that information destroyed; or

   (3) have a record appended to the information detailing the reasons for the challenge.

6. A data controller has reasonable grounds to deny a request under this article if –

   (1) satisfying the request will breach conditions of access to information imposed under section 4 of article 8 and the providing administration provides reasonable grounds to continue those conditions of access;

(2) satisfying the request will impede the effective application, investigation or prosecution of customs law;

(3) satisfying the request will reveal aspects of the risk-management process which would enable the subject or others to take steps in future to defeat the risk-management process; or

(4) providing the requested information would require a substantial and unreasonable amount of collation or research.

7. Each state party shall appoint a competent authority to whom a person may appeal any decision made by the data controller.

### *J Damages and Penalties*

Article 14 listed below and s 14 enable individuals to obtain compensation for any damage suffered as the result of the misuse of shared information.

Liabilities

Article 14

1. Every person shall be entitled to seek compensation through a competent judicial authority for damage suffered through the misuse by a customs administration or official of information it has obtained under this Convention.
2. A customs administration shall be liable in accordance with its national law for damage caused to an entity through the misuse by a customs administration or official of information it has obtained under this Convention.
3. For the purposes of this article, misuse means –
   (1) the use of information for purposes other than those specified in paragraph 1 of article 1;
   (2) wilfully relying upon information known or suspected to be untrue;
   (3) wilfully providing information known or suspected to be untrue and not providing an accompanying statement to this effect; or
   (4) unauthorised disclosure.
4. Each state party concerned shall agree on the terms and conditions of reimbursement for the damage caused if each state party concerned agrees that damage has occurred and the damage has not been referred to a competent judicial authority.
5. If each state party concerned agrees that damage has occurred but they are unable to agree on compensation, then either state party may request a recommendation on terms and conditions for compensation from the Administrative Committee.
6. Any legal costs incurred by a state party under this article shall be borne by the liable state party.

Sections 15 and 16 set out offences and penalties for breaches of the Model Law. The penalties are to be decided by the state implementing the Model Law.

15. Offences in relation to the improper disclosure of information

(1) Every person commits an offence who –

(a) discloses information received under this Act to a person or organisation not authorised to receive that information;

(b) discloses information received under this Act that is known or suspected to be incorrect without also providing a statement of that knowledge or suspicion;

(2) Every person who commits an offence against this section is liable on conviction to [Insert penalty].

16. Offences in relation to information disclosure intended to cause harm

1. Every person commits an offence who discloses information under this Act to a person or organisation not authorised to receive that information or otherwise uses that information with the intent of causing harm –

(a) to the subject of that information; or

(b) to the source of that information.

2. Every person who commits an offence against this section is liable on conviction to [Insert penalty].

### *K Administration*

The remaining articles and sections in the legal framework set out the rules for the management of information-sharing through this Convention. Article 15 establishes an administrative committee to set standards, settle disputes and promote the purposes of the Convention with other international bodies. Article 16 allows disputing state parties to present their arguments to the administrative committee. Prior to presenting the argument, they may choose to accept the administrative committee's decision as binding. If the Administrative Committee cannot resolve the dispute, the state parties will refer the dispute to state diplomatic representatives. This is a norm in other international agreements.[770]

[770] Christoph H Schreuer *The ICSID Convention: A Commentary* (Cambridge University Press, Cambridge UK, 2001), at 414; Nairobi Convention, above n 114, art 14 and 2004 Model Agreement, above n 549, para 30.

Article 17 contains the process for a state to register reservations against the Convention. Reservations against art 5, art 8 para 3, and art 15 are prohibited.[771] Amendments to the text of the Convention are provided for in art 18. Amendments require a majority vote of the state parties. Article 19 names the WCO as the depository for the Convention. Article 20 establishes when the Convention will enter into force. Articles 21 and 22 allow states to accede to, or retire from, the Convention once it is in force.

## *III Chapter Summary*

The legal framework proposed in this Chapter combines the needs of customs administrations for intelligence-sharing that were discussed in Chapter Two with explicit protection of the privacy and other human rights that were discussed in Chapters Three and Four.

This Chapter has discussed each of the articles of the proposed Convention and the sections of the Model Law. They were written to meet the intelligence-sharing needs of customs agencies and to demonstrate that the terms for managing information can be explicit even when the information and the ways in which it is used remain secret. The legal framework supports the claim that customs administrations can share intelligence through the transactional single window system and at the same time show how privacy and other human rights are treated. Chapter Four explained that the secret nature of intelligence information prohibits the knowledge and consent of the data subject in intelligence exchanges. This means that the Privacy Principles of Collection Limitation, Use Limitation and Individual Participation cannot be fully implemented. Nonetheless, terms were included in the legal framework that implemented the Privacy Principles as far as is practicable.

A draft of this Convention was provided to New Zealand experts in intelligence, law enforcement, policy and privacy. Those people were then interviewed to gauge the suitability of this Convention for its stated purposes. Those interviews are discussed in the next Chapter.

[771] Article 5 prevents manipulation of the intelligence-sharing process to interfere with trade, art 8(3) requires the protection of intelligence from unauthorised disclosure and art 15 establishes the administrative committee.

# Chapter Seven – Evaluation of the Proposed Legal Framework

This Chapter supports the claim that a legal framework can allow customs administrations to share intelligence through the transactional single window system and at the same time shows how privacy and other human rights are treated. It does so by evaluating the proposed legal framework against the measures that were established in Chapter Five to assess whether existing information-sharing agreements would be suitable for this purpose. Using the same measures allows a direct comparison with the other agreements and models for information-sharing that were examined in Chapter Five. This evaluation shows that the proposed legal framework is a better approach to sharing customs intelligence through the single window than the agreements that were examined.

There are seven Parts in this Chapter. Part I describes the interviews that took place following the preparation of the first draft of the Convention to confirm that it was practical and fit for purpose.

Parts II to V discuss the elements of the legal framework that relate to the measures established in Chapter Five. Feedback from the interviewees provide useful contextual information and is included in these Parts. Part VI examines alternative implementation methods that were suggested by interviewees. Part VII summarises the assessment of the legal framework against the same measures that were used in the evaluations of the other agreements and models that were examined.

## *I The Interviews*

This Part describes the interviews that were conducted with ten government agency staff members to test the suitability of the legal framework. Feedback was sought from twelve New Zealand customs and intelligence experts and ten responded. The experts commented on whether the draft framework contained what they viewed to be the essential elements and whether they thought the framework would be practical and effective. The stakeholders that were canvassed are representative of the interests of the small New Zealand border security intelligence operation. The interviewees held leadership positions in their particular fields and they were chosen for their accessibility and their ability to provide insightful comment on whether the legal framework would be appropriate for their needs. The interviews were not the basis of the Convention, but rather provided valuable information that helped ensure the legal framework would be acceptable and fit for purpose. The analysis in this Chapter benefits from the feedback provided in these interviews.

The purpose of the interviews was to confirm that the legal framework would be pragmatic and fit for purpose. The interviews were not intended or used as an empirical research method to derive evidence or to develop specific elements of the framework. The interviews provided assurance over reasoning applied in the development of the legal framework. They gave confidence that the legal framework provided a practical method for electronically sharing customs intelligence through a single window system. University ethics approval was granted for the consent form and questions included in Appendix One.

Opinions were sought through an interview process from intelligence users, legal counsel, policy advisors, senior managers, and privacy advocates. Each interviewee held a leadership role in a law enforcement, security or policy agency. The interviews consisted of free-flowing conversations around a series of structured questions relating to the proposed legal framework and its relationship to past approaches. The purpose of the interviews was not to extract cultural and socio-legal understanding of trust and confidence issues relating to customs intelligence. Nonetheless, interesting comment on that was offered and noted. Nine interviews occurred in face-to-face meetings and one interview was conducted by telephone. Two sets of questions were prepared for these interviews. The first set of questions covered matters relating to international intelligence-sharing arrangements. These questions were used with interviewees who had an intelligence or law enforcement background. The second set of questions were specific to the Privacy Principles and were used in discussions with all interviewees, including those with policy and legal expertise. The questions are listed in Appendix One. The interviewees were invited to take the conversation on divergent paths and to discuss connected concepts and ideas. These broader discussions provided the interviewer with a broad perspective of the customs intelligence and law enforcement operations. Feedback from the interviewees covered a range of topics such as the political environment, likely implementation issues, privacy treatment and the evidential use of intelligence.

The feedback was generally supportive. No one who was interviewed declined to answer any questions, nor were any of the responses obstructive, reticent or noncommittal. None of the individuals who were interviewed was opposed the Convention or its purpose. Several of the individuals suggested improvements to the Convention. Where appropriate, those suggestions have been included in the Convention and in the Model Law that was subsequently prepared to implement the Convention.

As a condition of participating in these interviews, each interviewee was promised anonymity for themselves and for their employer. Interviewees are referred to by number in the remainder of this Chapter. They were provided with the opportunity to review the notes made of their interviews and the inclusion of their comments in this work. Every

effort has been made to omit sensitive or classified intelligence materials or techniques from this work

## *II Enabling Trust between States and State Autonomy*

This Part discusses those aspects of the proposed legal framework that enable trust between states. Trust was identified in Chapter Two as an essential element of intelligence-sharing relationships. Seven interviewees said that trust between state parties will be a key factor in its implementation.[772] Interviewee Three said that trust between the individuals involved was essential and intelligence-sharing arrangements were often built on these personal relationships. These personal relationships enable intelligence with a low security classification to be shared by telephone because the personnel involved in the exchange are able to easily identify each other.[773]

Interviewee Three stated that it would be problematic to share intelligence with failed states because corruption and even state participation in organised crime make the appropriate handling of intelligence questionable. It should be noted that the level of government ineffectiveness necessary to be deemed a failed state varies between observers and the declaration that a state has "failed" can be controversial and carry significant political and economic consequences. Accordingly, the discussion with the Interviewee about failed states was based on general perceptions rather than any official declaration.[774]

By way of illustration, consider drug crime intelligence shared with Afghanistan. Afghanistan is arguably a failed state.[775] Its economy contributed 80% of the world's illicit opium in 1990, according to the United Nations.[776] Its government is currently challenged with:[777]

> …. criminality, insecurity, weak governance, lack of infrastructure, and the Afghan Government's difficulty in extending rule of law to all parts of the country ….

[772] All Interviewees except Interviewees Seven and Eight.

[773] Anderson, above n 210, at 148, identified that these personal cooperatives relationships also exist in the policing context.

[774] See also Patrick Stewart "Failed States and Global Security - Empirical Questions and Policy Dilemmas" (2007) 9(4) International Studies Review 644, at 644, for a discussion on the perception of failed states.

[775] Foreign Policy Group "The Failed State Index 2011" (17 June 2011) Foreign Policy Group <www.foreignpolicy.com>.

[776] United Nations "Afghanistan and the United Nations" (15 January 2015) United Nations <www.un.org>.

[777] Central Intelligence Agency "South Asia: Afghanistan" (24 June 2014) Central Intelligence Agency <www.cia.gov>.

Afghanistan has a well-publicised history of corruption and allegations of government involvement in drug trafficking.[778] Sharing intelligence with Afghanistan that includes information about drugs and organised crime could expose sensitive information about enforcement personnel, investigations and techniques used by criminals. An intelligence-sharing arrangement with a failed state such as Afghanistan would damage trust in intelligence-sharing relationships with other states.

Another factor affecting trust is that a third-party state may also be motivated to use trade intelligence it has received for its own economic gain and to the detriment of the supplying state. For example, a third-party state might receive intelligence that brings into question the integrity of food goods being exported. The third-party state might then take advantage of that information by initiating trade with the importing state. Such an act would economically disadvantage the exporting state and cause reputational harm to the intelligence-sharing system, especially if the intelligence later proved to be unreliable.

The following features A – D exist in the proposed Convention to promote trust between states.

### *A Information Access and Disclosure Control*

The proposed Convention and the Model Law impose controls to secure and ensure only authorised access to and disclosure of information in arts 8(3) and 8(4) and ss 7(1), 8(1), 8(8), 8(9) and 11(2). These requirements also implement the Security Safeguards principle.

### *B Audit, Review or Self-Reporting of Compliance*

Provisions are included in art 13 and s 13 for the appointment of a data controller. The data controller is accountable for compliance with the terms of the legal framework and has the ability to conduct an audit. Interviewee Ten requested a provision for the audit of intelligence handling processes by intelligence providers. This request was considered and not taken up because law enforcement and other intelligence handling agencies are unlikely to allow third parties to access their intelligence processing systems.

### *C Information Retention and Destruction Controls*

Although the Privacy Principles do not include a stipulation for information retention, the OCED Privacy Framework says:[779]

---

[778] James Risen and Mark Landler "Accused of Drug Ties, Afghan Official Worries U.S." *The New York Times*, at A1, at A1 and Matthew RosenBerg and Azam Ahmed "U.S. Aid to Afghans Flows On Despite Warnings of Misuse" *The New York Times* (New York, 30 January 2014), at A12.

[779] OECD Privacy Framework, above n 12, at 45 and 115.

> [O]pinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a clear dividing line between the level of basic principles or objectives and lower level "machinery" questions which should be left to domestic implementation….
>
> The Guidelines do not contain a data retention principle although many privacy regimes do. The implications of data persistence are nonetheless significant – whether it is the effect on an individual's reputation, the unanticipated and unauthorised uses of data, or the threats from breaches or malware to increasing amounts of data that is stored indeterminately.

The OECD Privacy Framework notes that there are increased risks to information when it is retained indefinitely.[780] A retention principle has been included in the New Zealand's domestic law.[781] For this reason, the legal framework contains rules in art 10 and s 10 that limit the retention of information to the period in which that information is useful. These rules include a review of the information every six months and the destruction of any personal information that is no longer essential for a criminal investigation or prosecution, the risk-management of on-going trade transactions, or the maintenance of accurate and complete records of decisions. The rules in art 11 and s 10 also require customs administrations to keep information up to date and correct. They must notify the recipients of information of changes that must be made to maintain the accuracy of that information. Customs administrations must correct or destroy information if they are requested to do so by the provider of that information.

### *D Voluntary, Not Compulsory, Information-sharing*

The main feature of the proposed legal framework that addresses the issues relating to trust is the ability to withhold information about the existence of intelligence that might otherwise be shared. An exclusion in the OECD Privacy Framework enables information to be withheld or Privacy Principles to not apply for "national sovereignty, national security and public policy", but in the EU Data Protection Directive it is more explicitly written as:[782]

> public security, defence, State security (including economic well-being of the State when the processing operation relates to State security matters) and the activities of the state in the area of criminal law.

[780] At 88, 91 and 115.

[781] Privacy Act 1993 (New Zealand), s 6 Principle 9.

[782] OECD Privacy Framework, above n 12, at 14 and Directive 96/9/EC, above n 634, art 3(2).

The EU "criminal law" exclusion is more specific than the "public policy" exclusion which appears in the OECD Privacy Framework. However, the OECD Privacy Framework includes commentary that indicates an acceptable exclusion for criminal investigations.[783] Other implementations of the Privacy Principles are similarly more explicit. For example, the Privacy Act 1993 (New Zealand) includes an exclusion "to avoid prejudice to the maintenance of the law" and the Privacy Act 1988 (Australia) has an exclusion for, among other things "unlawful activity, or misconduct of a serious nature".[784]

This ability to voluntarily share or withhold information is enabled by art 1 and ss 5(6) and 9 in the legal framework. These provisions provide a participating state with autonomy by allowing it to deny the existence of, and withhold, any intelligence for any reasons, including national interest.

### *III Transparency for the Privacy Principles*

This Part discusses the manner in which the Privacy Principles have been transparently implemented in the legal framework. The Interviewees provided much feedback on the concept of privacy generally and on the specific terms included in the legal framework.

Of those who commented on it specifically, four interviewees agreed that the OECD Privacy Framework provides the privacy principles that would most likely be widely accepted.

An interviewee also pointed out that Clean Slate Act in New Zealand has implications for the implementation of the Privacy Principles in the legal framework because Internet search engines do not comply with the legislated timeframes to "forget" criminal convictions.[785] Accordingly, how will other states treat information that should be expunged by the Clean Slate, when that information remains in the public domain? These are questions for a privacy debate that cannot be resolved through this legal framework. For the purposes here, the definition of personal information commonly used in the EU agreements is elaborated.[786] The EU's definition of personal data as "all information

[783] At 56.

[784] Privacy Act 1993 (New Zealand), s 6 Principle 2 (d) and Privacy Act 1988 (Australia), s 16A.

[785] Criminal Records Act 2004 (Clean Slate Act) (New Zealand). The Clean Slate Act is New Zealand legislation that expunges an individual's criminal history if they were convicted of a crime and had a non-custodial sentence (among other criteria) more than 7 years ago, and they have had no further convictions in the intervening period.

[786] For example, see "Definitions" in any of Economic Partnership Agreement, European Union – Suriname, above n 608; Economic Partnership, Political Coordination and Cooperation Agreement, European Union – Mexico OJ L276/44 (2000); Trade Agreement, European Union – Denmark and Faroe Islands OJ L53/1 (1996); or Agreement Establishing an Association, European Union – Algeria OJ L265/1 (2005).

relating to an identified or identifiable individual" is made more explicit to avoid divergent interpretations.[787] The definition of privacy used in the schedule of the proposed Convention was adapted from the Privacy Act 1988 (Australia) and the Official Information Act 1982 (New Zealand) (OIA) as follows:[788]

> (a) for natural persons, means information or an opinion, whether true or not, about or from an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion;
>
> (b) for artificial legal persons, information that can reasonably be considered prejudicial to the commercial position of the person who is the subject of the information; …

### *A Collection Limitation*

The Collection Limitation principle is one that can only be partially satisfied because intelligence is sometimes collected without the subject's knowledge and consent. Knowledge and consent wherever possible are required by art 12 and ss 5(2)(a) and 12(1).

### *B Data Quality*

The Data Quality principle is implemented through provisions that require customs administrations to keep information accurate and up to date. Customs administrations are also required to advise changes to those customs administrations with which they have shared that information. These terms are contained in arts 3, 10 and 11 and s 10.

Two of the interviewees stated that the reliability of intelligence shared through any system is an issue. It was suggested that a reliability rating system such as the Admiralty System could be employed to qualify and grade the intelligence.[789] The proposed legal framework does not specifically include a system for rating the reliability of intelligence. Nonetheless, a reliability rating system could easily be included in the WCO standards for information to be shared. WCO standards, such as the WCO Data Model, are indicated in art 3 and s 6.

### *C Purpose Specification*

The proposed Convention and the Model Law implement the Purpose Specification principle through text in art 1(1) and s 3 that clearly sets out the purposes for sharing the information. However, some of those purposes might not be the explicit reason for which

---

[787] Ibid.

[788] Privacy Act 1988 (Australia), s 6 and Official Information Act 1982 (New Zealand), s 9(2)(b).

[789] The Admiralty System is a system for grading the quality of intelligence, by reliability of source and by credibility of the information. For a discussion on the Admiralty System see McDowell, above n, at 209 and Joseph and Jeff Corkill (4th Australian Security and Intelligence Conference, Edith Cowan University, 5 -7 December, 2011), at 99.

the information was collected. For example, information that was collected to facilitate a trade transaction may later be used in a risk-management process, investigation or a prosecution. Nevertheless, this principle can be considered properly implemented because law enforcement exclusions have been put in place.

### *D Use Limitation*

The Use Limitation principle is implemented through the same text in the proposed Convention and the Model Law as for the Purpose Specification principle. There are provisions in art 8 and s 5(7) which prevent customs administrations from using shared information for anything but the purposes set out in art 1(1) and s 3 respectively. Customs administrations are also prevented by art 7 and ss 8(6) and 9(1)(e) from sharing information if they believe it will be used for another purpose.

### *E Security Safeguards*

Requirements to secure and protect information are imposed by art 8 and ss 8(1), 8(8), 8(9) and 11(2). These requirements implement the Security Safeguards principle. In this regard, the OCED Privacy Framework states:[790]

> Securing personal data has become a greater challenge. Individuals are exposed to increased potential harms including the risk of identity theft. Data breach notification has become an increasingly important element of privacy oversight.

### *F Openness*

The privacy principle of Openness requires:[791]

> [A] general policy of Openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

The OECD Privacy Framework says that notification of data breaches should be made to the subject of information by the data controller in cases where the unauthorised disclosure of that information "is likely to adversely affect" that person.[792] It makes more sense that this responsibility lies with the customs administration which would first discover the breach. Accordingly, in this legal framework a customs administration must advise any unauthorised disclosure to the customs administration which provided the information and, if an adverse effect is likely, the subject of the information. These

[790] OECD Privacy Framework, above n 12, at 67.

[791] At 15.

[792] At 16.

requirements are specified in art 8 and s 7(6). The same "adverse effect" condition is required for notification of breaches to the subject of the information. This is because reasons might persist for keeping the existence of the information secret if an adverse effect from the unauthorised disclosure is unlikely.

### *G Individual Participation*

The purpose of the Individual Participation principle is to enable individuals to access and challenge personal data.[793] The OECD Privacy Framework and its Expert Group consider this "as perhaps the most important privacy protection safety".[794] In art 13 and s 13 this is implemented through text that allows for individuals to challenge and to correct the information that is held about them through the data controller. Individuals may also challenge the accuracy of information that is presented in judicial processes under art 6 and s 8.

Where information must be kept secret from the individual, the customs administration has the responsibility to keep that information accurate and up to date through the Data Quality provisions.

In this regard, the legal framework includes provisions for individuals to query information held about themselves. These provisions are limited where there is a need to keep the existence of information secret. The establishment and role of the data controller are stipulated and the other policies and practices relating to personal data are clear. While the existence of secret information must remain secret, the rules ensure that personal information will be protected, carefully maintained and used only for explicit purposes. These rules are not secret. This openness can create public confidence in the information processing by the customs administrations.

An interviewee suggested that natural persons should not be charged costs for the collation and supply of any information held about themselves. That view was considered and rejected in favour of the approach taken in the OIA.[795] Although an individual has the right to access and see information about themselves, customs administrations, like many other government agencies, can hold decades of information relating to an individual and their transactions. Compiling and reporting that information could require a lot of time and resources. The OIA recognises that the effort needed to research and collate such personal information can be extensive and allows the fixing of charges for

[793] At 58.

[794] Ibid.

[795] Section 18(1).

that effort on a case-by-case basis.[796] Consequently, art 13 and s 13 allow the data controller to pass on the actual cost of that research and collation.

#### *H Accountability*

The Accountability principle is satisfied through the inclusion of terms in art 13 and s 13 which establish the role of the data controller. Accountability for compliance with the legal framework lies both with the customs administration and the data controller. For this reason, the data controller has the authority to conduct compliance audits. Offences have been created in ss 15 and 16 to enable the prosecution of customs officials or other persons who unlawfully or otherwise misuse information.

### *IV Transparent Protection for Other Human Rights*

There is a requirement in art 7 and s 7(5)(c) that all information that is shared has been obtained lawfully. This requirement provides some protection against the sharing of information that is gained through arbitrary search and seizure, torture or other cruel or inhuman treatment. This requirement also helps to implement the Collection Limitation principle.

Two interviewees raised issues about privacy and the lawful collection of information. They spoke about the treatment of incidentally or accidentally acquired intelligence. One example given included intelligence that was observed while executing a search warrant on another matter. That intelligence may relate to an offence outside the jurisdiction of customs, or an offence in another state. In this circumstance does the customs administration have the authority to keep and share this intelligence? Depending on the circumstances, that information may not be used in a New Zealand judicial process if it is deemed improperly obtained evidence.[797] Nevertheless, that information becomes knowledge that a customs administration could use to guide other investigations to lawfully obtain evidence. In New Zealand, the authority to share this information overseas is provided by the Customs and Excise Act 1996.[798] Foreign customs administrations would be similarly challenged to lawfully obtain information upon which

[796] Section 15(1A), but a government agency can exercise discretion and such charges are generally waived.

[797] Evidence Act 2006 (New Zealand), above n 296, s 30. For examples, see *R v Hawea* [2009] NZCA 127 in respect to a three-tier approach to the admissibility of confessional statements, see *R v McGaughey* [2007] NZCA 411 in respect of improperly obtained mobile phone text messages and see *R v Williams* [2007] NZCA 52 in respect of evidence obtained where the warrant to conduct the search had been procured cynically and for an ulterior purpose and *Hamed v R* [2011] NZSC 101, a case which the Supreme Court ruled on the admissibility of video surveillance as evidence. Prior to the Evidence Act 2006, a balancing approach was introduced in *R v Shaheed* [2002] 2 NZLR 377 (CA) for evidence obtained in breach of the New Zealand Bill of Rights Act 1990. The subsequent development of that balancing approach is discussed in Simon Consedine "R v Shaheed: The First Twenty Months" (2004) 10(1) Canterbury L Rev 77.

[798] Sections 281 (3)(b) and 282(1)(l).

to commence judicial proceedings. This issue is relevant as it impinges on the individual's right to privacy using the general exclusion for law enforcement purposes that exists in most privacy legislation.

## *V Enabling Intelligence-sharing for Customs Risk-management*

This Part discusses the features of the proposed Convention and Model Law that enable intelligence-sharing through a single window system. It explains how the components of the legal framework enable intelligence-sharing through a single window system.

### *A Terms that Enable Intelligence-sharing*

This intelligence-sharing purpose is set out in art 1 and referred to in s 3. The purpose is to enable a participating customs administration to share information for "applying, investigating, or prosecuting breaches of customs law, for risk-management and for the prevention of customs offences".

One interviewee suggested that the principal purposes of the Convention should be "managing risk, collecting revenue and managing compliance with domestic and international law". The suggestion related to the draft preamble that was provided to the interviewees prior to the discussion. The preamble has since been updated to reflect the importance of the Convention in managing legal compliance, economic, social and security interests. The wording of the purpose in art 1 has not changed though, as the current wording aligns closely with the wording accepted in past bilateral and multilateral agreements.[799] The interviewee also believed that the wording of art 1 appeared reactive rather than proactive and should include terms such as forecasting, foreseeing, or predicting non-compliance. The wording of art 1 was left unchanged because it is believed that those terms fit within "risk-management" which is included as a purpose.

Another interviewee shared a belief that the legal framework could be used as a model for establishing intelligence-sharing relationships between government agencies within New Zealand. That interviewee also believed that intelligence-sharing between government agencies within a state ensures the connectedness of government responses.

A third interviewee stated that the legal framework should enable the sharing of intelligence only for specific purposes such as an operational activity and not for non-operational activities such as a strategy report. This requirement is met through the wording of arts 1 and 2 and s 6. The wording of those provisions ties the notification and sharing of intelligence to the processing of a trade transaction.

[799] For example, the Cooperative Arrangement between Customs Authorities, Japan – United States of America (1997), above n **Error! Bookmark not defined.**, art 4 and Cooperative Arrangement between Customs Authorities, New Zealand – Australia (2006), above n 551, s 1.

### *B Common Standards/Format for Information Exchange*

The requirement to use common standards and formats for the exchange of intelligence information is set out in art 3 and s 6(3).

### *C Terms that Enable Real-Time Electronic Exchange*

The mechanism for the electronic exchange of information in real-time as set out in art 3 and s 6(3). The legal framework requires that a customs administration sends an electronic notification of the existence of intelligence that may be shared along with the trade transaction information through a single window system. The purpose of a single window system is to exchange trade transaction information electronically.

## *VI Other Implementation Options*

The proposed legal framework is intended to enable the automation of existing intelligence-sharing arrangements. It uses a single window system as the vehicle for information exchange. Its terms can supplant the information-sharing provisions in existing multilateral and bilateral agreements, enabling states to use their single window systems to exchange intelligence electronically, rather than their existing manual processes. The terms will provide greater visibility of the treatment of personal information in intelligence exchanges.

There are also opportunities for this approach to be implemented in new intelligence-sharing arrangements. Any endeavour to create new, cooperative intelligence relationships could be challenged by factors including differences in economic power, political alignment, and culture, as described in Chapter Two. Although the legal framework does not provide solutions to resolve those differences, some interviewees shared their views on the ways they believed the provisions might be implemented in new intelligence-sharing agreements. Those views are discussed in this sub-part. They align well with the overview of factors influencing intelligence cooperation in Chapter Two.

Options for implementation include establishing the proposed Convention with a global scope under the auspices of an international body such as the WTO. Alternatively, an interviewee said that regional cluster arrangements such as trading blocs may be a more successful vehicle for the implementation of this approach. This is because they operate in common areas of interest such as trade, drug crime and terrorism. It was suggested that that regional arrangements could evolve over time to become more global in scope. Regional clusters such as APEC, ASEAN and the Five Eyes are more likely to share intelligence assessments and holdings because of their common interests and an already established high level of trust, said the interviewee. An opportunity for a regional

approach was also recognised in the policing context by Anderson, prior to the establishment of Europol, the EU police cooperation organisation.[800]

One interviewee pointed to the Five Eyes security and intelligence partnership as an example of trusted relationships enabling the sharing of intelligence. Another interviewee stated that the relationship of the same five countries in the Five Eyes agreement is the basis upon which new identity information-sharing agreements have been established for immigration purposes. The interviewee claimed that these agreements have been written to include the privacy protection principles.[801] The immigration agreements were examined and were found to be similar to the Convention proposed here in that they specify information exchange for a particular purpose and have controls to implement the Privacy Principles. However, these immigration agreements are different to the proposed Convention because they are intended to establish a sharing arrangement for fingerprint data. The immigration system is designed to share information on individuals who have already been assessed as a high risk of being non-compliant with immigration law.[802] The system also limits state parties to a maximum of 30,000 information requests each year.[803] Intelligence-sharing takes place using manual processes when triggered by fingerprint matches.

An interviewee observed that there are "big differences" in the levels of trust between some regions. Three interviewees suggested that the lack of established trust would be an obstacle to implementation on such a global scale. These views correspond to the analysis in Chapter Two. States are unlikely to have a need or an interest in sharing trade intelligence with states with which they have no strong economic or political ties. There will be less direct benefit to states sharing trade intelligence with a non-trading-partner states. This is because neither state will be able to share risk-management information about its traders that would be useful to the other state. Moreover, it could create a

[800] Anderson, above n 210, at 169–171.

[801] Immigration New Zealand "Five Country Conference Questions and Answers" (20 December 2010) Immigration New Zealand <www.immigration.govt.nz>. The extent to which the immigration information-sharing arrangements between New Zealand and Australia satisfy the Privacy Principles, and the residual privacy risks are evident in the Immigration New Zealand "Privacy Impact Assessment for Exchange of Information between the New Zealand Department of Labour and the Australian Department of Immigration and Citizenship, as part of the Five Country Conference High Value Data Sharing Protocol" (2010) Immigration New Zealand <www.immigrastion.govt.nz>. See also United Kingdom Home Office "Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference" (2010) United Kingdom Home Office <www.gov.uk>.

[802] Immigration New Zealand, above n 801, at 2.

[803] At 7.

liability for the sharing state under its domestic law because sharing intelligence without an explicit purpose contravenes the Purpose Specification and Use Limitation principles.

It was suggested that a model for implementation much like the one used for PNRGOV could be used. The interviewee said that the PNRGOV system relies on the WCO to establish and maintain the PNRGOV framework; ICAO endorses and publishes the formal PNRGOV standards; and PNRGOV implementation is managed through the existing working relationships of the IATA members. It was argued that the legal framework proposed here could similarly use the WCO, the WTO and regional trading blocs like APEC as vehicles for implementation. The WCO could manage and maintain the framework and standards, the WTO could sponsor the Convention and implementation could then occur through regional trading blocs like APEC and ASEAN. It was submitted that implementation through regional clusters like APEC is likely to occur faster than it would through a larger body like the WTO or WCO. The interviewee believed that a Convention established at the WTO would be more successful than one made through the WCO because agreements made at the WTO are "more binding". It was also pointed out that the WTO had the power to impose penalties whereas the WCO is a cooperation environment which "has no powers to bind or compel". For this reason, implementation under the auspices of the WTO could improve the compliance of states with the terms of the legal framework. One of the interviewees said that, as a global approach, the Convention proposed here would be less likely to achieve widespread implementation if it were promoted solely under the auspices of bodies such as the UN.

Two interviewees recommended increasing the scope of this legal framework to include the purposes of all border agencies, such as immigration and biosecurity. They claimed that that would aid its acceptance. That idea was not taken up because broadening the purposes would challenge the principles of Purpose Specification and Use Limitation. It would also be likely to result in extended periods of data retention because information would be held until there was certainty that all its potential uses had expired.

Interviewee Three suggested that the INTERPOL system could be used instead of this approach to share intelligence. That idea was not taken up for two main reasons. Firstly, the INTERPOL system holds information in a central database which is accessible by all member states.[804] Secondly, the INTERPOL system issues particular types of notices, such as to arrest and extradite criminals or to locate missing persons, and it can be queried for further information.[805] The INTERPOL system does not automatically associate information for risk-assessment with trade transaction information. As such, it is less

[804] INTERPOL, above n 713.

[805] Ibid.

suitable for the purposes of the legal framework, which proposes tagging trade transactions with a flag that indicates the existence of intelligence information.

It was suggested by an interviewee that there might be issues with "quid pro quo expectations" for implementation in developing states. This corresponds to the concept of symmetric intelligence-sharing discussed in Chapter Two. The interviewee suggested that issues may also arise if a wealthier state that has less concern for human rights chooses to exert influence on developing states through donations of aid, in other words an asymmetric relationship. This issue is one for the making of international agreements generally and not an issue that is particular to the context of this work. Consequently, no terms are proposed to address this issue.

It is recommended that the use of this legal framework beyond existing intelligence-sharing relationships should follow the approach of a Convention sponsored by the WTO. The administrative framework and rules should be managed by the WCO. Implementation will be best achieved through regional trading blocs like ASEAN that share common interests with regard to economic growth, security and the suppression of crime.[806] Regional implementations should adopt the WCO mandated Convention so that, over time, all customs intelligence-sharing arrangements apply the same standards.

## *VII Chapter Summary*

This Chapter has shown that a legal framework with the explicit treatment of privacy and other human rights can allow customs administrations to share intelligence through the transactional single window system.

The proposed legal framework was evaluated against the measures that were established in Chapter Five. The evaluation showed that the proposed legal framework is a better model for sharing customs intelligence through the single window than the other models that were examined.

Comment from the New Zealand customs and intelligence experts interviewed was that the legal framework would provide a practical and effective method for sharing intelligence through a single window system. Their feedback was used to fine tune the provisions and support the analysis in this Chapter. The analysis has shown that the approach proposed here is well suited to sharing intelligence through a single window system.

[806] For example see Jurgen Haacke *ASEAN's Diplomatic and Security Culture: Origins, Development and Prospects* (Routledge, Birmingham, 2013), at 52; Pacific Disaster Centre "Regional Risk Assessment for ASEAN Member States" (21 April 2015) Pacific Disaster Centre <www.pdc.org> and Canadian Associates to Develop Democratic Burma "Parliamentarians Call on ASEAN to Address Rohingya Crisis" (22 April 2015) Euro-Burma Office <www.euro-burma.eu>.

The extent to which the proposed legal framework satisfies the requirements for sharing intelligence through the single window is summarised in Table 11. Chapter Eight provides conclusions on the suitability of the legal framework.

**Table 11. Summarised assessment of the proposed legal framework**

| ***Theme*** | **Requirement** | **(✓) Meets<br>(P) Partially meets<br>(✗) Fails to meet** |
|---|---|---|
| *Trust between states that intelligence is secured, accessed and used appropriately* | Information access and disclosure control | ✓ |
| | Audit, review or self-reporting of compliance | ✓ |
| | Information retention and destruction controls | ✓ |
| *State autonomy* | Voluntary, not compulsory, information-sharing | ✓ |
| *Include the Privacy Principles* | Collection Limitation | P |
| | Data Quality | ✓ |
| | Purpose Specification | ✓ |
| | Use Limitation | ✓ |
| | Security Safeguards | ✓ |
| | Openness | ✓ |
| | Individual Participation | ✓ |
| | Accountability | ✓ |
| *Promote access to justice, prohibit information gained through arbitrary search and seizure and prohibit information gained through torture* | Information is collected lawfully | ✓ |
| *Implement intelligence-sharing through a single window* | Enables intelligence-sharing | ✓ |
| | Common standards/format for information exchange | ✓ |
| | Enables real-time electronic exchange | ✓ |

# Chapter Eight – Conclusion

This Thesis addressed the question: "What would a legal framework that enables customs administrations to share intelligence through a single window system look like?". The thesis proposes a legal framework for this purpose. The legal framework comprises a draft international Convention and a Model Law for domestic implementation.

The thesis has shown that, with a legal framework such as that proposed, the single window could be used to automate intelligence exchanges. The legal framework includes transparent terms for managing privacy to improve public confidence.

The logic of the thesis is that -

1. there is no law enabling customs to share intelligence electronically and in real-time for risk management purposes; and
2. the privacy principles of the OECD Privacy Framework are the most widely accepted expression of public expectations for the treatment of privacy; and
3. with some exceptions, the principles of the OECD Privacy Framework can be imposed as controls on a practical intelligence-sharing arrangement; and
4. making those controls transparent should improve public confidence; so
5. a legal framework that allows customs administrations to share intelligence through the transactional single window system, and at the same time show how privacy and other human rights are treated, should improve public confidence.

Chapters Two, Three and Four discussed the effect of secrecy and the publicity about human rights abuses on public confidence in government intelligence activity.

The criteria of a legal framework that would be suitable for sharing customs intelligence through a single window system were also examined in Chapters Two, Three and Four. The principles of the OECD Privacy Framework, were acknowledged in Chapter Four as the most widely accepted statement of public expectations for privacy.

The criteria for a legal framework that would be suitable for sharing customs intelligence were expressed as a set of measures in Chapter Five. The assertion that there is no existing law enabling customs to share intelligence electronically and in real-time for use in risk management processes was examined in Chapter Five.

In Chapter Six, a legal framework was proposed that implements, as far as practicable, the measures that were set out in Chapter Five. The legal framework was evaluated against those measures in Chapter Seven. Experts in New Zealand border security, intelligence and privacy were interviewed. They concluded that the legal framework would enable a practical and effective approach to sharing intelligence.

It was suggested that disclosing the terms for the treatment of privacy and other human rights would improve public confidence in intelligence-sharing arrangements. Transparency of these terms in domestic law and in an international Convention would enable greater public scrutiny and debate than is often possible for intelligence-sharing arrangements. The acceptability of these terms and the improvement in public confidence is predicted, but not proven. Nonetheless, transparency would enable the acceptability of the privacy terms in the legal framework to be tested in forums such as in parliament and the courts. This presents an opportunity for further research. The improvement in public confidence could be proven through an empirical study that measures confidence before and after the framework is implemented.

Another opportunity for further research was identified in Chapter Five. The analysis in that Chapter found that past multilateral agreements, for example the Nairobi Convention and the WCO Model Agreement, have not been well supported. Some reasons were offered for the lack of support, including resistance to the notion of central pools of intelligence and central oversight. However, not all the reasons for the lack of support are well understood. This warrants further investigation.

Although privacy is the human right most affected by the intelligence-sharing, personal information used by the state for national security and law enforcement purposes is often exempted from privacy law. Operational security requirements in this context can prevent the data subject from knowing or consenting to personal information that is being shared. The thesis shows that the Privacy Principles can be adapted to address this limitation and the blanket exemption of national security and law enforcement processes from privacy law is not necessary.

An implementation approach recommended by interviewees is for the legal framework to be adopted by an international organisation such as the WTO. The proposed Convention could then be used to set terms for the sharing of intelligence between trusted partners, such as exist in regional trading blocs. The Model Law would guide the development of domestic law to implement the terms of the Convention. In another approach, the terms of the legal framework would be used as a template to guide the development of future intelligence-sharing agreements. However, any approaches that involve creating intelligence cooperation would need to overcome barriers to trust such as cultural, security, economic and political differences. The proposed legal framework may not provide ways to reconcile those differences.

There is no existing law that enables customs to share intelligence electronically and in real-time for risk management purposes. The legal framework proposed in this thesis would serve that purpose. It has explicit controls for the protection for human rights, including the principles of the OECD privacy framework. The legal framework is designed to make these controls apparent to enable public scrutiny and to improve public confidence.

This thesis proposes a legal framework to enable intelligence to be shared through a single window system with transparent terms for managing human rights. The legal framework is practicable and superior to the current approaches to customs intelligence-sharing in which the protection of human rights is seldom evident. The implementation of the proposed legal framework would give members of the public confidence that, even though some information that is exchanged under a single window system using this framework must be kept secret, the terms for protecting human rights in that exchange are clear.

The conclusion is that the proposed legal framework allows customs administrations to share intelligence through a single window system and shows how privacy and other human rights can be treated in a way that should improve public confidence in the customs intelligence-sharing process.

# Appendix One – Interviews

This Appendix lists the questions that were asked of the interviewees referred to in Chapter Seven. The feedback from the interviewees led to improvements in the proposed Convention. The numbering of articles and sections changed as a result of those improvements so the article and paragraph references in these questions are no longer correct.

Interviewees in intelligence and law enforcement operations or intelligence analysis roles were asked both sets of questions. Interviewees in legal counsel and policy roles were asked only the second set of questions. Each interview took place over 1 to 2 hours. These interviews involved free-flowing discussions that were loosely structured around the questions below. Open questions enabled the interviewees to take the discussion down divergent paths to provide the interviewer with the broadest possible perspectives.

# *I Consent Form*

**VICTORIA UNIVERSITY OF WELLINGTON**
**CONSENT TO PARTICIPATION IN RESEARCH**

**Title of project:**
Research into an International Law for
Sharing Trade Risk-management Information
in Support of the Trade Single Window

I have been given and have understood an explanation of this research project. I have had an opportunity to ask questions and have them answered to my satisfaction.

I understand I may withdraw myself (or any information I have provided) from this project at any time following my interview and before I am provided material to review, or within one month from when I am provided material to review. I may withdraw without having to give reasons and without penalty of any sort.

I understand that any information I provide will be kept confidential to the researcher and his supervisors. I understand the published results will not use my name and no information nor opinions will be attributed to me or my organisation in any way that will identify me, unless I specifically give my consent to do so. I understand that any written interview notes will be transcribed electronically and then the written records shall be securely destroyed by cross-cut shredding. I understand the electronic records of interviews will be securely erased three years after the completion of the PhD unless I indicate that I would like them returned to me.

- ☐ I acknowledge that no information or opinions which I have shall be attributed to me in any reports on this research.
- ☐ I acknowledge that no information or opinions which I have shall be attributed to my organisation in any reports on this research.
- ☐ I would like the records of my interview returned to me at the conclusion of the project.
- ☐ I understand that I will be provided a draft copy of anything in the thesis that cites or quotes information I have provided, for my review and approval.
- ☐ I understand that the data I provide will not be used for any other purpose or released to others without my written consent.
- ☐ I would like to receive a summary of the results of this research when it is completed.
- ☐ I agree to take part in this research.

Signed:

Name of participant _____ (Please print clearly) _____ Date:

## *II Interview: Usefulness to Intelligence Users*

The draft Convention aims to:

(a) encourage more cooperation for information-sharing for trade risk-management; and

(b) provide protection to the personal information and human rights of individuals.

Part I describes the information that can be shared and the method of sharing. Part II applies some limits on the information that can be shared and how it may be used. Part III requires states to ensure the confidentiality of information is maintained. It also mandates requirements for accuracy, retention and the timely disposal of information. Part IV requires states to have systems in place to allow individuals to access and correct information about them, except where that information must be kept secret. Part V sets out administrative rules for the Convention.

1. Privacy: The Convention includes conditions for the treatment of personal information. Would this treatment be impractical? What changes would you suggest to the privacy requirements to make the Convention more useful for information-sharing? (refer to Articles 8 to 13)

2. Right of refusal: The Convention states that information-sharing for trade risk-management is consensual, not obligatory, and it provides grounds under which the supply of information might be refused. One of these grounds is where a state has registered a "Reservation", meaning it will not be bound by one or more conditions of the Convention. Are these grounds for refusal appropriate? Are there too many or not enough reasons for refusing to share information? How is this likely to be a barrier to information-sharing? What changes would you suggest? (refer to Articles 1(3), 4 & 7)

3. Managing the information and its confidentiality: The Convention includes conditions for securing, managing and maintaining the accuracy of the information that is shared. Would these conditions provide you with enough confidence to share trade risk-management information with another administration/agency? Would you find compliance with these conditions too onerous? What changes would you suggest to make these conditions more useful? (refer to Articles 5 to 10 and 13(6))

4. Process: The Convention provides for a process of sharing information for trade risk-management, keeping it up to date, and disposing of it when it is no longer required. The process does not require the maintenance of a centralised database of shared information that all states can access. Are these measures appropriate? Are they practical? Why would you, or why would you not, want to have a single international database that all states could access for this information-sharing? What changes would you suggest to make the process more useful or practical? (refer to Articles 2, 3, 9, 10 & 11)

5. Administration and non-compliance: The Convention contains administrative conditions and provisions for addressing non-compliance. Do you believe the administrative conditions are appropriate? Can you suggest more effective means of managing information-sharing for trade risk-management? Is the system for addressing non-compliance appropriate? What changes would you suggest? (refer to Articles 14 to 20)

6. Implementation: What barriers to the implementation of this Convention would you envisage? Would this Convention make it easier or harder to improve international cooperation in information-sharing for trade risk-management? How could this Convention be improved to increase international adoption?

7. Are there any other comments or suggestions you would like to make?

## *III Interview: Privacy*

The draft Convention aims to:

(a) encourage more cooperation for information-sharing for trade risk-management; and

(b) provide protection to the personal information and human rights of individuals**.**

Part I describes the information that can be shared and the method of sharing. Part II applies some limits on the information that can be shared and how it may be used. Part III requires states to ensure the confidentiality of information is maintained. It also mandates requirements for accuracy, retention and the timely disposal of information. Part IV requires states to have systems in place to allow individuals to access and correct information about them, except where that information must be kept secret. Part V sets out administrative rules for the Convention.

The provisions of the draft Convention have been written with the requirements of the OECD privacy guidelines in mind.[807] This has been done with the knowledge that:

(a) no internationally recognised standard for privacy protection exists; and

(b) for this Convention to be adopted by at least the OECD states, it must comply with the minimum requirements stipulated in the guidelines.

Considering this, in your opinion:

1. Are the OECD guidelines sufficient to provide sufficient protection for the privacy of individuals, or should other guidelines be adopted?

2. Does the draft Convention provide adequate controls in respect of the Collection Limitation principle of the OECD guidelines? If not, what other controls would you recommend? (refer to Articles 7 & 12)

   (Collection Limitation principle stated here)

[807] OECD "Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data" (1980) OECD <www.oecd.org>.

3. Does the draft Convention provide adequate controls in respect of the Data Quality principle? If not, what other controls would you recommend? (refer to Articles 1, 5, 7, 9, 10 & 11)

(Data Quality principle stated here)

4. Does the draft Convention provide adequate controls in respect of the Person Specification Principle? If not, what other controls would you recommend? (refer to Articles 1(2), 2 & 12)

(Purpose Specification principle stated here)

5. Does the draft Convention provide adequate controls in respect of the Use Limitation principle? If not, what other controls would you recommend? (refer to Articles 1(2), 3, 4, 7(1), 9 & 12)

(Use Limitation principle stated here)

6. Does the draft Convention provide adequate controls in respect of the Security Safeguards principle? If not, what other controls would you recommend? (refer to Articles 4, 7(4) & 8)

(Security Safeguards principle stated here)

7. Does the draft Convention provide adequate controls in respect of the Openness principle? If not, what other controls would you recommend? (refer to Articles 12 & 13)

(Openness principle stated here)

8. Does the draft Convention provide adequate controls in respect of the Individual Participation principle? If not, what other controls would you recommend? (refer to Articles 12 & 13)

(Individual Participation principle stated here)

9. Does the draft Convention provide adequate controls in respect of the Accountability principle? If not, what other controls would you recommend? (refer to Article 13)

(Accountability principle stated here)

The OECD guidelines also include Four Basic Principles of International Application for the free flow of information and legitimate restrictions.[808]

10. Do Articles 1(4), 4, 8 & 9 include appropriate measures in accordance with the first Basic Principle listed below? What changes would you recommend?

(First Basic Principle stated here)

11. Does Article 8 include reasonable and appropriate steps in accordance with the second Basic Principle listed below? What changes would you recommend?

(Second Basic Principle stated here)

12. Do Articles 4, 7, 8 and 9 include appropriate controls in accordance with the third Basic Principle listed below? What changes would you recommend?

(Third Basic Principle stated here)

13. Are there any Articles in the draft Convention that would create obstacles or exceed requirements, as per the fourth Basic Principle listed below? What changes measures would you recommend?

(Fourth Basic Principle stated here)

14. Are there any other comments or suggestions you would like to make?

[808] The questions relating to the Four Basic Principles of International Application were based on the principles in the OECD "Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data", which were published in 1980. Shortly after the interviews were completed, these principles were amended in OECD Privacy Framework, above n 12, published in July 2013.

# Appendix Two – Proposed Convention

This Convention is discussed in Chapter Six. It follows the format of the Vienna Convention on the Law of Treaties.[809] It has a preamble, followed by numbered articles, sections, subsections, and paragraphs. Definitions are included in a schedule.

This Convention provides a prototype for an international agreement to enable the exchange of intelligence information between the State Parties to the Convention.

International Convention for Information-sharing for the
Risk-management of International Trade

PREAMBLE

The State Parties to this Convention,

Recognising that trade risk-management enables the more efficient facilitation of trade and accurate identification of customs offences;

Aspiring to the trade facilitation and security benefits that can be achieved by exchanging information between the single window systems of State Parties;

Recalling the information requirements of UN/CEFACT Recommendation No.33, the Recommendation and Guidelines on establishing a single window;

Having regard to the Customs Co-operation Council Recommendation on Mutual Administrative Assistance made in December 1953, the World Customs Organisation Declaration on the Improvement of Customs Co-operation and Mutual Administrative Assistance made in June 2000 and the Resolution on Security and Facilitation of the International Trade Supply Chain, adopted in June 2002 by the Customs Co-operation Council;

Acknowledging the commitments of states to promote universal respect for human rights and fundamental freedoms under the United Nations Charter, the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights; and

Desiring to make an effective international agreement for sharing information for trade risk-management,

Have agreed as follows:

[809] Vienna Convention on the Law of Treaties 1155 UNTS 331 (1969).

## Scope and Purpose of the Convention

### Article 1

1. This Convention shall apply where a state party through its customs administration shares information with the customs administration of another state party for the purposes of applying, investigating, or prosecuting breaches of customs law, for risk-management and for the prevention of customs offences.

2. Any intelligence-sharing carried out under this Convention is voluntary and no providing administration shall be compelled to provide intelligence related to any trade transaction.

3. Any information shared under this Convention shall be used by the requesting administration for the purposes listed in paragraph 1 and shall not be used for any other purpose unless expressly permitted by the providing administration.

4. Each state party to this Convention undertakes to take the necessary steps, in accordance with its constitutional processes to adopt such laws or other measures as may be necessary to implement the provisions of this Convention.

5. The Schedule lists the meanings of the expressions used in this Convention.

## Information covered by this Convention

### Article 2

1. The information that may be shared under this Convention includes –

   (1) information related to any entity that is information about –

      (a) past criminal convictions;

      (b) any on-going criminal investigation or prosecution;

      (c) any known or suspected association with criminal activity;

      (d) any known or suspected association with past offenders or criminal organisations;

      (e) any customs offence that is known or suspected to be in progress or about to be committed;

      (f) past trade transactions related to that entity which may show a trend of compliance or non-compliance with customs law;

(2) information related to any trade transaction that is –

(a) useful for the accurate recordkeeping of the transaction;

(b) useful to the evaluation of the accuracy of other information specific to the trade transaction or related to any entity; or

(c) useful to establishing an accurate classification of any entity for the assessment of compliance with customs law including correct revenue collection; and

(3) any other information that is relevant to risk-management, trade facilitation and customs law enforcement or risk-management techniques that may be adopted.

2. The providing administration shall provide intelligence information relating to entities to the extent possible and to the extent permissible under the national laws of the State Parties.

Information-sharing process

Article 3

1. Providing administrations may share specific information in advance of the departure of goods from their territories.

2. To reduce duplication in information-sharing, the following procedures will apply –

(1) The providing administration may include with the information related to any trade transaction a declaration that intelligence exists which may be shared;

(2) The requesting administration may request all the intelligence that may be shared if –

(a) the requesting administration has not previously been provided with the intelligence holding; or

(b) the intelligence has been previously provided and has been destroyed under article 10.

(3) The providing administration shall provide the date that an update was last made to the intelligence that may be shared.

(4) The requesting administration may request the update to the intelligence if that update has not previously been received.

(5) The providing administration shall provide the intelligence or the update as requested by the requesting administration.

3. All requests, notices and other information shared under this Convention shall be transmitted electronically using standards for data type and format published by the World Customs Organisation for this purpose.

Information-sharing where a reservation applies

Article 4

1. The providing administration shall consider the effect of any reservation made by the requesting state party to the articles of this Convention.

2. The providing administration shall refuse to provide information if it is unable to ensure to its own satisfaction that the purpose of the requested information is for a public good that outweighs the potential harm that may result from a reservation made by the requesting state party.

3. A providing administration shall inform the requesting administration of the reasons for any refusal to provide information pursuant to paragraph 2 of this article.

Untrue Information

Article 5

1. No state party shall share information that it knows or suspects to be untrue without also sharing a statement of that suspicion.

2. No state party shall share information that it knows or suspects to be untrue for the purpose of interfering with the legitimate trade of another state party.

3. State Parties shall take reasonable steps to validate provided information to ensure legitimate trade is not inhibited by information that is known or suspected to be untrue.

Judicial application

Article 6

State Parties shall ensure that the subject of any application, investigation or prosecution of customs law that relies upon information shared under this Convention shall have access to a process by which the subject may challenge the accuracy of the information.

## Limitation of shared information

### Article 7

1. State Parties shall limit the information that is shared under this Convention to information which can be reasonably considered relevant to the purposes specified in paragraph 1 of article 1.

2. A providing administration shall not share information that it knows or suspects to have been obtained by unlawful means.

3. A requesting administration shall not accept information that it knows or suspects to have been obtained by unlawful means.

4. A providing administration shall not share information that it knows or suspects to have been requested for any purpose inconsistent with the purposes of this Convention.

## Confidentiality

### Article 8

1. Information shared under this Convention shall be treated as confidential by the customs administrations of the territories from which the goods will depart, through which transshipment occurs and in which the goods will arrive.

2. Any intelligence shared under this Convention shall be used only by the officials of the requesting state party and shall not be disclosed to any other state party, customs administration, organisation or person except with the express permission of the providing administration.

3. The requesting administration shall limit access to the provided information to officials for the purposes specified in paragraph 1 of article 1.

4. The requesting administration shall protect provided information to prevent unauthorised disclosure.

5. The requesting administration shall adopt such additional conditions for access to, use of, storage, transmission, correction and destruction of intelligence as may be required by the providing administration.

6. A providing administration shall not impose unreasonable or unnecessary conditions for access to, use of, storage and transmission of information.

7. The requesting administration shall disclose to the providing administration a summary of the protection afforded to the provided information on the first occasion information is provided and at least annually thereafter.

8. The requesting administration may use intelligence provided under this Convention as evidence in a prosecution or in support of any other judicial process.

9. To enable compliance reviews or audits the requesting administration shall record each access to the provided information and that record shall contain the date and time the information was accessed, the details of the person or persons accessing the information and the reason or purpose for accessing the information.

10. The providing administration shall ensure the transmission of information to a requesting administration is secured against unauthorised disclosure.

11. The providing administration shall refrain from providing information including intelligence to a requesting administration if the requesting administration fails to observe the terms of this Convention.

12. The requesting administration shall give notice of any unauthorised disclosure of information and the steps that have been or will be taken to remedy that situation to the providing administration and wherever possible to the subject of the information if that subject is likely to be adversely affected.

Special provisions for transshipment information

Article 9

1. Any information other than intelligence shared under this Convention may be disclosed to any official of another state party where that information relates to a transshipment and the disclosure is –

   (1) compliant with any conditions required by the providing administration pursuant to paragraph 5 of article 8;

   (2) to a state party which has within its territory a transshipment point for the goods; and

   (3) for the purposes specified in paragraph 1 of article 1; or

   (4) to facilitate the transshipment.

2. The requesting administration shall impose the terms of article 8 upon any agency or official of any other state party to which it discloses provided information under this article.

Correction, retention and destruction of information

Article 10

1. The requesting administration may indefinitely retain any personal information it has been provided if that information is essential for –

   (1) a criminal investigation or prosecution;

   (2) the risk-management of on-going trade transactions; or

   (3) the maintenance of accurate and complete records of decisions.

2. The requesting administration shall destroy any personal information included in provided information within six months of that information being received if the information is not essential for a purpose described in paragraph 1 of this article.

3. The requesting administration shall review the provided information every six months and destroy any personal information that is no longer deemed essential.

4. A providing administration may at any time require the correction of information it has provided to the requesting administration, and –

   (1) upon receipt of such a request, the requesting administration shall without delay record the correction to the information it has been provided; or

   (2) if the requesting administration must maintain an original record of the information that was provided, it shall record a reference to the correction it has received as an addendum to the original record.

5. The providing administration may at any time require the destruction of intelligence it has provided to the requesting administration.

6. Upon receipt of a request from a providing administration to destroy intelligence that it has provided, the requesting administration shall without delay destroy all records of that intelligence.

7. State Parties shall ensure that every organisation or person has access to a process by which they may view and correct any information other than intelligence about themselves which is shared under this Convention.

## Maintaining accuracy

### Article 11

1. For the first six months after providing information, a providing administration shall inform the requesting administration of any addition, correction or erasure which is necessary to keep that information accurate, complete and up to date.

2. Six months after information was first provided and if the information is essential for a purpose described in paragraph 1 of article 10, a requesting administration may request an update to the information from the providing administration from time to time if warranted by the particular circumstances.

## Notice to the subjects of information

### Article 12

1. State Parties shall inform the subjects of the information at the time it is collected that the information may be shared under this Convention, except where informing the subject is not possible or for compelling reasons of public good.

2. For the purposes of paragraph 1 of this article, compelling reasons of public good are –

   (1) that informing the subject will impede the effective application, or investigation or prosecution of a breach of customs law; or

   (2) that informing the subject will reveal aspects of the risk-management process that would enable the subject or others to take steps in future to defeat the risk-management process.

## Data Controller

### Article 13

1. Each state party shall appoint an official of its customs administration as a data controller to be accountable for compliance with the terms of this Convention.

2. The data controller shall have the authority to conduct compliance audits of the information processing systems of the customs administration periodically at his or her discretion.

3. Any organisation or person shall have the right to request from the data controller confirmation of whether or not the customs administration has information relating to that organisation or person.

4. Any organisation or person shall have the right to request and be provided any data related to that organisation or person –

   (1) within a reasonable time;

   (2) at a cost that does not exceed the actual cost of researching and collating the information; and

   (3) in a form that can be reasonably expected to be understood by that organisation or person.

5. Any person may challenge the accuracy of the information relating to that person and –

   (1) have that information corrected;

   (2) have that information destroyed; or

   (3) have a record appended to the information with details of the correction.

6. A data controller has reasonable grounds to deny a request under this article if –

   (1) satisfying the request will breach conditions of access to information imposed under section 4 of article 8 and the providing administration provides reasonable grounds to continue those conditions of access;

   (2) satisfying the request will impede the effective application, investigation or prosecution of customs law;

   (3) satisfying the request will reveal aspects of the risk-management process which would enable the subject or others to take steps in future to defeat the risk-management process; or

   (4) providing the requested information would require a substantial and unreasonable amount of collation or research.

7. Each state party shall appoint a competent authority to whom a person may appeal any decision made by the data controller.

## Liabilities
### Article 14

1. Every person shall be entitled to seek compensation through a competent judicial authority for damage suffered through the misuse by a customs administration or official of information it has obtained under this Convention.

2. A customs administration shall be liable in accordance with its national law for damage caused to an entity through the misuse by a customs administration or official of information it has obtained under this Convention.

3. For the purposes of this article, misuse means –

   (1) the use of information for purposes other than those specified in paragraph 1 of article 1;

   (2) wilfully relying upon information known or suspected to be untrue;

   (3) wilfully providing information known or suspected to be untrue and not providing an accompanying statement to this effect; or

   (4) unauthorised disclosure.

4. Each state party concerned shall agree on the terms and conditions of reimbursement for the damage caused if each state party concerned agrees that damage has occurred and the damage has not been referred to a competent judicial authority.

5. If each state party concerned agrees that damage has occurred but they are unable to agree on compensation, then either state party may request a recommendation on terms and conditions for compensation from the Administrative Committee.

6. Any legal costs incurred by a state party under this article shall be borne by the liable state party.

## Administration
### Article 15

1. There shall be an Administrative Committee –

   (1) to consider issues relating to the administration and implementation of this Convention;

(2) to consider disputes and issue recommendations or binding decisions to the State Parties concerned;

(3) to recommend to State Parties uniform interpretations of the terms of this Convention;

(4) to maintain relations with other international bodies for the purpose of keeping this Convention in harmony with other customs, law enforcement and trade related initiatives;

(5) to recommend amendments to this Convention to State Parties; and

(6) to consider any other issues of relevance to this Convention.

2. The members of the Administrative Committee shall consist of ten experts of high moral standing.

3. The Administrative Committee shall be elected from a list of persons nominated by the State Parties.

4. Each state party may nominate one representative from its own nationals.

5. Elections of the Administrative Committee shall be held triennially at a meeting of the World Customs Organisation.

6. The term of the Administrative Committee shall be three years.

7. Two thirds of the State Parties to this Convention shall constitute a quorum for the election.

8. The inaugural election shall occur not later than six months after the date this Convention enters into force.

9. At least three months prior to each election, the State Parties shall notify their nominated representatives to the World Customs Organisation.

10. If for any reason a member of the Administrative Committee can no longer perform his or her duties, the state party which nominated that representative shall appoint another representative from among its nationals to serve for the remainder of the term, that appointment being subject to the approval of not less than six members of the Administrative Committee.

11. Representatives may be re-elected.

12. The Secretary-General of the World Customs Organisation or a duly appointed delegate shall chair the inaugural meeting of the Administrative Committee.

13. The Administrative Committee shall elect its officers from amongst its members.

14. The Administrative Committee shall establish its own rules subject to this Convention.

15. The rules of the Administrative Committee shall establish when and how polls shall be taken for the purpose of amending the articles of this Convention.

16. The Administrative Committee shall determine the staff and facilities necessary for the effective performance of its duties.

17. The expenses of the Administrative Committee meetings, staff and facilities shall be shared equally amongst the State Parties.

18. The expenses of each Administrative Committee member shall be borne by the state party that nominated the member.

19. The rules of the Administrative Committee shall establish when and where meetings are to be held.

## Disputes
## Article 16

1. Without prejudice to paragraph 1 of article 15, any dispute between State Parties concerning the interpretation of any part of this Convention shall be settled by negotiation.

2. Any dispute that cannot be settled through negotiation shall be referred to the Administrative Committee which shall consider the dispute and issue a recommendation.

3. The Administrative Committee shall examine in closed session the arguments and evidence of the State Parties in dispute.

4. The Administrative Committee shall issue a written statement of its findings and recommendations to the State Parties in dispute.

5. The State Parties in dispute may agree in advance to accept the recommendations of the Administrative Committee as binding.

6. The Administrative Committee is exempt from any liability in respect of its findings and recommendations.

7. Disputes for which no resolution is found shall be settled by diplomatic means.

## Reservations and exemptions

### Article 17

1. The following articles or paragraphs may not be, in whole or in part, subject to reservations –

   (1) Article 5;

   (2) Article 8 paragraph 3; and

   (3) Article 15.

2. A state party that has entered a reservation may withdraw or amend it at any time by providing a notification to the Administrative Committee specifying the date and time the withdrawal or notification is to take effect.

3. Any information may be withheld or the provision of information may be delayed if there are grounds to believe that providing the information will impede an on-going investigation, prosecution or law enforcement operation. In such a case, the providing administration shall consult with the requesting administration to determine whether the information can be provided, subject to such additional terms and conditions as the providing administration may specify.

4. Information may be withheld if the providing administration deems the effort needed to provide the information outweighs the potential benefits that can be gained from the information.

## Amendments

### Article 18

The articles of this Convention may be amended by majority vote of the State Parties.

## Depository

### Article 19

This Convention, all signatures with or without reservation and all instruments of ratification shall be deposited with the Secretary-General of the World Customs Organisation.

## Entry into Force

### Article 20

1. This Convention shall enter into force three months after ten State Parties have signed the Convention with or without reservation and have deposited their instruments of ratification.

2. State Parties shall enact national law to implement the terms of this Convention.

## Accession

### Article 21

This Convention shall remain open for accession by any State. The instruments of accession shall be deposited with the Secretary-General of the World Customs Organisation.

## Denunciation

### Article 22

1. This Convention is of unlimited term but any state party may denounce it at any time after its entry into force.

2. The denunciation shall be notified in writing to the Administrative Committee, who shall deposit the denunciation with the Secretary-General of the World Customs Organisation.

3. The denunciation shall be effective upon notification to the Administrative Committee.

SCHEDULE

Definitions

1. For the purposes of this Convention –

"Administrative Committee" means the committee described in article 15.

"customs administration" means an agency of the state party established to ensure that craft or goods crossing into the territory of that state comply with customs law of that state;

"customs law" means any legal and administrative provisions applicable or enforceable by the customs administration in connection with the importation, exportation, transshipment, transit, storage and movement of goods, including legal and administrative provisions relating to measures of prohibition, restriction, and control of, and in connection with combating money laundering;

"customs offence" means any violation or attempted violation of customs law;

"entity" means any party to a trade transaction, or any location, means of transport, business or any other physical thing or abstract concept that can be related directly or indirectly to the trade transaction and for which there is information useful to the risk-management of the trade transaction;

"information" means any data in any format that may be obtained from the public domain, or directly from the parties to the trade transaction, or from any other sources to which the state party has access;

"intelligence" means verifiable or unverifiable information related to the trade transaction or an entity which is considered relevant to risk-management and of which the existence, possession or use of such information is deemed a secret by the providing state party;

"official" means any customs officer or other government agent designated by a state party to apply customs law;

"party to the trade transaction" means the exporter, the importer, or any other person or organisation involved in the processing or transit of the trade transaction;

"person" means both natural and artificial legal persons;

"personal information" –

(a) for natural persons, means information or an opinion, whether true or not, about or from an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion;

(b) for artificial legal persons, means information that can reasonably be considered prejudicial to the commercial position of the person who is the subject of the information;

"provided information" means information shared between customs administrations;

"providing state party" means the state party whose customs administration is requested to provide information;

"providing administration" means the customs administration from which information is requested;

"requesting administration" means the customs administration which requests information;

"requesting state party" means the state party whose customs administration requests information;

"reservation" has the same meaning as defined and used in the Vienna Convention on the Law of Treaties (1969) 1155 UNTS 331;

"risk-management" means any process by which a customs administration evaluates information to establish the possibility of a customs offence;

"State party" means a state that has signed and ratified the Convention.

"trade transaction" means the processes involved in the cross-border movement of goods from the point of export to the point of import;

"transshipment" means the transfer of goods from one carrier or vessel to another at an intermediate destination while those goods are in transit from the point of export to the point of import;

"unauthorised disclosure" means the release of any provided information to any other state party, customs administration, organisation or person where that information is not available in the public domain and where the disclosure has not been explicitly permitted by the providing administration;

2. Other terms used in this Convention have the same meanings as in the World Customs Organisation Data Model.

# Appendix Three – Model Law

This Model Law is discussed in Chapter Six. It follows the format used for New Zealand domestic legislation in that it has a table of contents and an interpretation section, followed by numbered sections, subsections, paragraphs and subparagraphs. It differs from the UNCITRAL template for Model Laws such as UNCITRAL Model Law on Cross-Border Insolvency 1997 and UNCITRAL Model Law on International Commercial Arbitration 1985, each of which has a preamble and numbered articles.

This Model Law provides a prototype for a national law that gives effect to the obligations made under the proposed Convention for Information-sharing for the Risk-management of International Trade (the Convention).

CONTENTS


1. Title 248
4. Interpretation 248
2. Purpose 248
3. Primacy of the Act 249
4. Interpretation 248
5. Principles 249
6. Information that may be shared 251
7. Disclosure of Information 252
8. Confidentiality of information disclosed 253
9. Reasons for not disclosing information 255
10. Correction, retention and destruction of information 256
11. Requesting information 257
12. Notice to the subjects of information 258
13. Data controller 258
14. Liabilities 259
15. Offences in relation to the improper disclosure of information 260
16. Offences in relation to information disclosure intended to cause harm 260
17. Administration 261
18. Disputes 261

## 1. Title

This Act is the Intelligence-sharing through Single Window Implementation Act.

## 2. Interpretation

(1) In this Act –

"Customs administration" means the [Insert Customs Agency] and its private contractors which enforce the state's law regarding the flow of goods and other material through its borders.

"Convention" means the Convention for Information-sharing for the Risk-management of International Trade;

"customs purpose" means a purpose described in section 3.

"misuse" means –

(a) the use of information for purposes other than those listed in section 3;

(b) wilfully relying upon information known or suspected to be untrue;

(c) wilfully providing information known or suspected to be untrue and not providing an accompanying statement to this effect; or

(d) unauthorised disclosure; or

(e) modifying information to make it untrue or to mislead a risk-assessment, investigation or prosecution.

"WCO Data Model" means the information framework first published by the World Customs Organisation as the WCO Customs Data Model in January 2002 and updated from time to time to standardise and simplify customs data requirements.

(2) Unless otherwise stated, all other terms used in this Act have the same meaning as in the Convention.

## 3. Purpose

(1) The purpose of this Act is –

(a) to establish controls for [Insert Customs Agency] to share information with other customs administrations for the purposes of applying,

investigating, or prosecuting breaches of customs law, for risk-management and for the prevention of customs offences; and

(b) to establish effective protection for the rights of individuals in accordance with the state's obligations in domestic and international law.

(2) When interpreting this Act, the following must be considered –

(a) the principles and purposes of this Act; and

(b) the Convention.

**4. Primacy of the Act**

(1) This Act applies to the exclusion of any provision in any other legislation that prohibits, restricts or authorises the [Insert Customs Agency] to disclose information to or receive information from another customs administration.

(2) Nothing in this Act limits or otherwise restricts any other legislative requirement for the customs administration to disclose information.

**5. Principles**

(1) The interpretation of this Act must favour the presumption that the human rights and privacy of individuals are observed, except where required by law.

(2) Every person's right to privacy is protected according to the following principles –

(a) Personal data shall be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the subject of that information;

(b) All personal data collected shall be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, shall be accurate, complete and kept up to date;

(c) The purposes for which personal data are collected shall be specified not later than at the time of data collection;

(d) Personal data shall not be disclosed, made available or otherwise used for purposes other than a customs purpose, except –

(i) with the consent of the subject of that information; or

(ii) by the authority of law; and

(e) Personal data shall be protected against loss or misuse.

(3) A person shall have the right –

(a) to obtain confirmation from the [Insert Customs Agency] of whether or not the customs administration has data relating to the person;

(b) to be informed of data relating to him or her within a reasonable time –

(i) at a charge, if any, that is not excessive;

(ii) in a reasonable manner; and

(iii) in a form that is readily intelligible to the person;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to the person and if the challenge is successful to have the data erased, rectified, completed or amended.

(4) Personal data may be retained indefinitely if that data are essential for –

(a) a criminal investigation or prosecution;

(b) the risk-management of on-going trade transactions; or

(c) the maintenance of accurate and complete records of decisions.

(5) Personal data included in provided information will be destroyed within six months of that information being received if the information is not essential for a purpose described in paragraph (3) of section 10.

(6) Any intelligence-sharing carried out under this Act is voluntary and [Insert Customs Agency] may not compel another customs administration to provide intelligence related to any trade transaction.

(7) Information shared under this Act shall be only be used for customs purposes and shall not be used for any other purpose unless expressly permitted in law or permitted by the providing administration.

## 6. Information that may be shared

(1) The information that may be shared under this Act includes information related to any trade transaction that is –

(a) described in the World Customs Organisation Data Model and other standards and recommendations published by the World Customs Organisation for the purposes of this Act;

(b) useful for keeping an accurate record of the transaction;

(c) useful to the evaluation of the accuracy of other information specific to the trade transaction or related to any entity; or

(d) useful to establishing an accurate classification of any entity for the assessment of compliance with customs law including correct revenue collection.

(2) Other information that may be shared under this Act includes information related to any entity that is –

(a) information about past criminal convictions;

(b) information about any on-going criminal investigation or prosecution;

(c) information about any known or suspected association with criminal activity;

(d) information about any known or suspected association with criminal persons or criminal organisations;

(e) information about any customs offence that is known or suspected to be in progress or about to be committed;

(f) information about past trade transactions related to that entity which may show a trend of compliance or non-compliance with customs law; or

(g) any other information that is relevant to risk-management, trade facilitation and customs law enforcement or risk-management techniques that may be adopted.

(3) The information shared under this Act shall be transmitted electronically using standards for data type and format published by the World Customs Organisation for this purpose.

**7. Disclosure of information**

(1) [Insert Customs Agency] shall only disclose information under this Act to the customs administrations of a state party.

(2) Before goods depart the territory of the state, [Insert Customs Agency] may disclose trade transaction information –

(a) to the customs administrations of the territories in which the goods will arrive; and

(b) to the customs administrations of any territories though which transshipment will occur.

(3) Along with the trade transaction information it discloses, [Insert Customs Agency] may provide notice that it holds intelligence that may be shared and the date that the intelligence holding was last updated.

(4) [Insert Customs Agency] may provide the intelligence or the update to the intelligence as requested by a requesting administration.

(5) [Insert Customs Agency] shall not –

(a) share information that it knows or suspects to be untrue without also sharing a statement of that suspicion; or

(b) share information that it knows or suspects to be untrue for the purpose of interfering with the legitimate trade of another state party; or

(c) share information that it knows or suspects to have been obtained by unlawful means.

(6) [Insert Customs Agency] shall give notification of any unauthorised disclosure of information and the steps that have or will be taken to remedy that situation to the providing administration and wherever possible to the subject of the information if that subject is likely to be adversely affected.

## 8. Confidentiality of information

(1) The customs administration shall –

(a) ensure the transmission of information to a requesting administration is secure from unauthorised disclosure;

(b) take reasonable steps to validate provided information to ensure legitimate trade is not inhibited by information that is known or suspected to be untrue; and

(c) ensure the requesting administration adopts any reasonable and necessary conditions for access to, use of, storage and transmission of provided information.

(2) On the first occasion information is provided and at least annually thereafter, [Insert Customs Agency] shall request from each requesting administration a summary of the protection afforded to provided information.

(3) Where it is known or suspected that a requesting administration is using provided information for any purpose other than a customs purpose, [Insert Customs Agency] must request that requesting administration –

(a) to cease using the information for purposes not specified in this Act; and

(b) to provide an affirmation that provided information will only be used for purposes specified in this Act.

(4) [Insert Customs Agency] may authorise a requesting administration to disclose provided information to another agency or person if –

(a) The functions of that agency or person include the prevention, investigation or prosecution of offences punishable by fines or imprisonment; and

(b) The information is disclosed subject to conditions stating –

(i) how that agency or person may make use of the information; and

(ii) the conditions for access to, use of, storage, transmission, correction and destruction of the information.

(5) Where it is known or suspected that a requesting administration has disclosed provided information to any party not authorised under paragraph (4) of this section, [Insert Customs Agency] must request that requesting administration –

(a) to cease disclosing provided information to any party other than those authorised by the customs administration;

(b) to confirm that provided information will not be disclosed to any other party unless authorised by the customs administration; and

(c) to provide evidence that any and all copies of the information disclosed to the unauthorised party have been destroyed; or

(d) to confirm that any and all copies of the information disclosed to the unauthorised party have been destroyed.

(6) If [Insert Customs Agency] considers that a requesting administration is unable or unwilling to prevent unauthorised disclosure or prevent the use of information for any purpose other than those specified in this Act, [Insert Customs Agency] must cease disclosing information to that requesting administration under this Act.

(7) For the disclosure of intelligence, [Insert Customs Agency] shall notify the requesting administration of any additional conditions for access to, use of, storage, transmission, correction and destruction of intelligence as may be required to ensure the security of the intelligence or to satisfy the requirements of the agency, body or person that supplied the intelligence to [Insert Customs Agency].

(8) [Insert Customs Agency] shall protect provided information to prevent unauthorised disclosure.

(9) [Insert Customs Agency] shall adopt such additional conditions for access to, use of, storage, transmission, correction and destruction of intelligence as may be required by the providing administration.

(10) If [Insert Customs Agency] is unable or unwilling to adopt the conditions required by a providing administration, it must refuse to receive the intelligence.

(11) [Insert Customs Agency] will not disclose intelligence received under this Act to any other state party, requesting administration, organisation or person except with the express permission of the providing administration.

(12) [Insert Customs Agency] will provide a summary of the protection afforded to provided information if such a summary is requested by a providing administration.

(13) Any information shared under this Act may be used as evidence in a prosecution or in support of any other judicial process.

(14) [Insert Customs Agency] will ensure that the subject of any application, investigation or prosecution of customs law that relies upon information shared under this Act has access to a process by which the subject may challenge the accuracy of the information.

## 9. Reasons for not disclosing information

(1) [Insert Customs Agency] may choose not to share information with the requesting administration of any state party if –

(a) any reservations that have been made to the Convention by that state party could result in a breach of the principles of this Act if such information is shared;

(b) it is unable to ensure to its own satisfaction that the purpose of the requested information is for a public good that outweighs the potential harm that may result from a reservation made to the Convention by that state party;

(c) laws or other measures as are needed to implement the provisions of the Convention are not in place in the territories of that state party;

(d) the requesting administration is not able to satisfy the customs administration that it can fulfil all the conditions for information access, use, storage, transmission, correction and destruction that may accompany that information;

(e) it becomes aware that the information may be used for a purpose or disclosed in a manner inconsistent with the purposes of this Act; or

(f) the information has previously been provided.

(2) [Insert Customs Agency] must not provide information to a requesting administration that fails to provide a summary of the protection to be afforded to provided information under section 8 paragraph (12).

(3) [Insert Customs Agency] may choose not to disclose intelligence nor disclose that it holds intelligence about any entity for –

(a) any reason it considers the state party or the requesting administration that would otherwise receive the intelligence may fail to protect or use the intelligence in accordance with the Convention; or

(b) any foreign policy, diplomatic or security reason.

(4) [Insert Customs Agency] must not disclose intelligence or disclose that it holds intelligence if doing so will impede the effective application, investigation or prosecution of a breach of the law.

**10. Correction, retention and destruction of information**

(1) [Insert Customs Agency] shall –

(a) update its information without delay when it becomes aware that the information it holds is inaccurate.

(b) The customs administration may retain a copy of any inaccurate information if it is essential for the maintenance of accurate and complete records of decisions.

(c) for the first six months after providing information, inform a requesting administration of any addition, correction or erasure which is necessary to keeping that information accurate, complete and up to date.

(d) retain provided information for no more than six months unless it is essential for a purpose described in paragraph (3) of this section.

(e) request updates to the intelligence elements of provided information as necessary from time to time during the period of retention to ensure that the information is accurate when used.

(f) inform a requesting administration of any addition, correction or erasure which is necessary to keeping that intelligence accurate, complete and up to date.

(g) if it becomes aware of any compelling reason that provided information must be destroyed –

(i) destroy that information without delay; and

(ii) notify the reason for which the information must be destroyed to any customs administration to which it has provided that information or from which it has received that information

and request that information be destroyed if warranted by the particular circumstances.

(2) [Insert Customs Agency] shall review the provided information every six months and destroy all personal information that is no longer deemed essential for a purpose described in paragraph (3).

(3) [Insert Customs Agency] may indefinitely retain any information it has been provided if that information is essential for –

(a) a criminal investigation or prosecution;

(b) the risk-management of on-going trade transactions; or

(c) the maintenance of accurate and complete records of decisions.

(4) Upon receipt of a request from a providing administration to correct information it has provided –

(a) [Insert Customs Agency] shall record the correction to the information it has been provided; or

(b) if [Insert Customs Agency] must maintain an original record of the information that was provided, it shall record a reference to the correction it has received as an addendum to the original record.

(5) Upon receipt of a request from a providing administration to destroy intelligence it has provided, [Insert Customs Agency] shall destroy all records of the intelligence.

**11. Requesting information**

(1) Following the receipt of trade transaction information from a providing administration, [Insert Customs Agency] –

(a) shall use the trade transaction information only for customs purposes;

(b) may request a copy of the intelligence if the trade transaction information includes a notification that a providing administration has intelligence relating to any entity which [Insert Customs Agency] has not previously received;

(c) may request a copy of the updated intelligence if a providing administration provides a notification that intelligence has been updated since it was last provided;

(d) shall limit its requests for intelligence to those which can be reasonably considered relevant for customs purposes; and

(e) must not accept information that it knows or suspects to have been obtained by unlawful means.

(2) [Insert Customs Agency] will for audit and compliance review purposes create a record of each access to the information it has been provided which contains the date and time the information was accessed, the details of the person or persons accessing the information and the reason or purpose for accessing the information.

**12. Notice to the subjects of information**

(1) [Insert Customs Agency] shall inform the subjects of the information at the time it is collected that the information may be shared under this Convention, except where informing the subject is not possible or for compelling reasons of public good.

(2) Compelling reasons of public good are –

(a) that informing the subject will impede the effective application, or investigation or prosecution of a breach of customs law; or

(b) that informing the subject will reveal aspects of the risk-management process that would enable the subject or others to take steps in future to defeat the risk-management process.

**Data controller**

(1) [Insert Customs Agency] shall appoint an official as a data controller to be accountable for compliance with this Act.

(2) The data controller shall have the authority to conduct compliance audits of the information processing systems of the [Insert Customs Agency] periodically at their discretion.

(3) Any person has the right –

(a) to request from the data controller confirmation of whether or not [Insert Customs Agency] has information relating to that person;

(b) to request and be provided by the data controller any data related to that person –

(i) within a reasonable time;

(ii) at a cost that does not exceed the actual cost of researching and collating the information; and

(iii) in a form that can be reasonably expected to be understood by that person.

(c) to challenge the accuracy of the information relating to that person and –

(i) have that information corrected;

(ii) have that information destroyed, unless the customs administration requires that information to be retained indefinitely for a purpose described in paragraph (3) of section 10; or

(iii) have a record appended to the information with details of the correction.

(4) A data controller may have reasonable grounds to deny a request under subparagraphs (a) and (b) of paragraph (3) if –

(a) satisfying the request will breach conditions of access to information imposed under section 8 paragraph (9) and the providing administration provides reasonable grounds to continue those conditions of access;

(b) satisfying the request will impede the effective application, investigation or prosecution of customs law;

(c) satisfying the request will reveal aspects of the risk-management process which would enable the subject or others to take steps in future to defeat the risk-management process; or

(d) providing the requested information would require a substantial and unreasonable amount of collation or research.

(5) A person who is dissatisfied with a decision of the data controller and who has reason to believe that it is erroneous in law or fact may appeal to the [Insert State's Privacy Commissioner, Ombudsman, or Similar Role].

## 13. Liabilities

(1) [Insert Customs Agency] shall be liable for damage or loss that occurs as the result of its unauthorised disclosure of personal information.

(2) [Insert Customs Agency] shall be liable for damage or loss caused to any person by the misuse of information obtained under this Act.

(3) Where [Insert Customs Agency] is liable for damage or loss to a person resident in the territories of another state party and that damage or loss has not been referred to a competent judicial authority, [Insert Customs Agency] shall agree the terms of reimbursement with the customs administration of the state party concerned.

(4) If no agreement can be reached then [Insert Customs Agency] may request a binding decision or non-binding recommendation on terms and conditions for compensation from the Administrative Committee.

(5) [Insert Customs Agency] must implement any binding decision on compensation it receives from the Administrative Committee.

(6) Where the Administrative Committee has issued a non-binding recommendation for compensation, [Insert Customs Agency] must –

(a) comply with the terms and conditions included in the recommendation; or

(b) refer the claim for loss or damage to a competent judicial authority in the territory of the state party concerned.

**14. Offences in relation to the improper disclosure of information**

(1) Every person commits an offence who –

(a) discloses information received under this Act to a person or organisation not authorised to receive that information;

(b) discloses information received under this Act that is known or suspected to be incorrect without also providing a statement of that knowledge or suspicion;

(2) Every person who commits an offence against this section is liable on conviction to [Insert penalty].

**15. Offences in relation to information disclosure intended to cause harm**

(1) Every person commits an offence who discloses information under this Act to a person or organisation not authorised to receive that information or otherwise uses that information with the intent of causing harm –

(a) to the subject of that information; or

(b) to the source of that information.

(2) Every person who commits an offence against this section is liable on conviction to [Insert penalty].

## 16. Administration

(1) [Insert Customs Agency] shall implement recommendations made by the Administrative Committee –

(a) on the scope and format for information-sharing;

(b) on the uniform interpretation of the terms from the Convention that are used in the application of this Act; and

(c) on issues relating to the administration and implementation of the Convention through this Act.

(2) If [Insert Customs Agency] chooses to nominate a representative for election to the Administrative Committee –

(a) the nominated representative must be a person of high moral standing who is an expert in customs risk-management or who has relevant legal experience; and

(b) [Insert Customs Agency] must notify the nominated representative to the World Customs Organisation at least three months prior to each election.

(3) If for any reason a representative of [Insert Customs Agency] who has been duly elected to the Administrative Committee can no longer perform his or her duties, [Insert Customs Agency] shall appoint another suitably qualified representative citizen to serve for the remainder of the term, that appointment being subject to the approval of not less than six members of the Administrative Committee.

(4) [Insert Customs Agency] shall set rules for and bear the expenses of its elected representative to the Administrative Committee.

## 17. Disputes

(1) In the event that [Insert Customs Agency] cannot agree with any other customs administration on the terms for sharing information or the interpretation of any part of the Convention, either party may refer the dispute to the Administrative Committee, and –

(a) [Insert Customs Agency] may choose in advance to accept any recommendation issued by the Administrative Committee as binding; and

(b) [Insert Customs Agency] shall hold the Administrative Committee exempt from any liability in respect of its findings and recommendations.

(2) Disputes for which no resolution is found shall be referred to diplomatic representatives.

# Bibliography

## *Treaties and International Agreements*


Agreement between Japan and the Republic of Indonesia for an Economic Partnership UNTS 2780 I-48935 (2007).

Agreement between the European Community and the Government of Canada on the Processing of Advance Passenger Information and Passenger Name Record Data OJ L82/15 (2006).

Agreement between the European Union and Australia on the Processing and Transfer of Passenger Name Record (PNR) Data OJ L186/4 (2012).

Agreement between the European Union and New Zealand on Cooperation and Mutual Administrative Assistance in Customs Matters COM(2016) 17 final (not signed or ratified).

Agreement between the Government of the United States of America and the Government of the Republic of Korea to Improve International Tax Compliance (2015) (not deposited, retrieved from www.treasury.gov).

Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records OJ L215/5 (2012).

Agreement Establishing an Association, European Union – Algeria OJ L265/1 (2005).

Agreement Establishing the ASEAN – Australia – New Zealand Free Trade Area UNTS 2672 I-47529 1 (opened for signing 27 February 2009).

Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Colombia OJ L354/2186 (2012).

Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Costa Rica OJ L346/1902 (2012).

Agreement for Mutual Administrative Assistance in Customs Matters, European Union – El Salvador OJ L346/1902 (2012).

Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Guatemala OJ L346/1902 (2012).

Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Honduras OJ L346/1902 (2012).

Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Nicaragua OJ L346/1902 (2012).

Agreement for Mutual Administrative Assistance in Customs Matters, European Union – Panama OJ L346/1902 (2012).

Agreement for Partnership and Cooperation, European Union – Kazakhstan OJ L196/1 (1999).

Agreement for Partnership and Cooperation, European Union – Kyrgyz Republic OJ L196/46 (1999).

Agreement for Partnership and Cooperation, European Union – Russia OJ L327/1 (1997).

Agreement for Partnership and Cooperation, European Union – Tajikistan OJ L350/1 (2009).

Agreement for Partnership and Cooperation, European Union – Uzbekistan OJ L229/1 (1999).

Agreement on a Customs Union and Common Economic Zone, Belarus – Kazakhstan – Kyrgyzstan – Tajikistan – Russia UNTS 2212 I-39320 103 (26 February 1999).

Agreement on Customs Cooperation and Mutual Assistance, European Union – Canada OJ L 7/37 (1997).

Agreement on Mutual Administrative Assistance in Customs Matters, European Union – China OJ L 375/19 (2004).

Agreement Regarding Mutual Customs Assistance, USA – Colombia UST LEXIS 134 (1999).

Border Services Agency Mutual Assistance Agreement, Japan – Canada (2005) (not deposited, retrieved from www.customs.go.jp/english/cmaa).

Charter of the United Nations and Statute of the International Court of Justice UNTS 1 (opened for signing 26 June 1945, entry into force 24 October 1945).

Convention Against Corruption UNGA Res 5/84 (31 October 2003).

Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Convention Against Torture) UNGA Res 39/46, A/Res/39/46 (1975).

Convention Against Transnational Organized Crime UNGA Res 55/25 (15 November 2000).

Convention between the Government of the French Republic and the Government of the United States of America for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income and Capital UNTS 1963 I-33537 (31 August 1994).

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ETS 108 (1981).

Convention for the Suppression of the Financing of Terrorism UNGA Res 54109 (9 December 1999).

Convention on International Trade in Endangered Species of Wild Fauna and Flora 993 UNTS 243 (1973).

Convention Relative to the Treatment of Prisoners of War (1950) 75 UNTS 135.

Cooperative Arrangement between Customs Administrations, New Zealand – South Korea (1992) (not deposited, provided to the author by the New Zealand Customs Service).

Cooperative Arrangement between Customs Authorities, Japan – United States of America (1997) (not deposited, retrieved from www.customs.go.jp/english/cmaa).

Cooperative Arrangement between Customs Authorities, New Zealand – Australia (2006) (not deposited, provided to the author by the New Zealand Customs Service).

Cooperative Arrangement between Customs Authorities, New Zealand – Hong Kong (1991) (not deposited, provided to the author by the New Zealand Customs Service).

Cooperative Arrangement between Customs Authorities, New Zealand – United Kingdom (1996) (not deposited, provided to the author by the New Zealand Customs Service).

Cooperative Arrangement between Customs Authorities, New Zealand – United States of America (1996) (not deposited, provided to the author by the New Zealand Customs Service).

Customs Assistance Agreement, United States – Mexico UST LEXIS 258 (2000).

Customs Co-Operation and Mutual Administrative Assistance Agreement, Japan – Hong Kong (2008) (not deposited, retrieved from www.customs.go.jp/english/cmaa).

Customs Union Agreement, European Union – Andorra OJ L374/13 (1990).

Economic Partnership Agreement, European Union – Antigua OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Bahamas OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Barbados OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Barbuda OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Belize OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Dominica OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Grenada OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Guyana OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Jamaica OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – St Christopher and Nevis OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – St Lucia OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – St Vincent and the Grenadines OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Suriname OJ L289/I/1 (2008).

Economic Partnership Agreement, European Union – Trinidad and Tobago OJ L 289/I/1 (2008).

Economic Partnership, Political Coordination and Cooperation Agreement, European Union – Mexico OJ L276/44 (2000).

European Convention for the Protection of Human Rights and Fundamental Freedoms ETS 5 (1950).

European Convention for the Protection of Human Rights and Fundamental Freedoms (The European Convention for Human Rights, or ECHR) UNTS 213 I-2889 222 (1950).

FATCA Agreement Model 1A IGA Reciprocal, Preexisting TIEA or DTC, 30 November 2014 (retrieved from www.treasury.gov).

Free Trade Agreement between New Zealand and the Republic of Korea (opened for signing 23 March 2015) (not deposited, retrieved from www.mfat.govt.nz).

Free Trade Agreement between the Government of New Zealand and the Government of the People's Republic of China UNTS 2590 I-46123 101 (2008).

International Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offences (Nairobi Convention) UNTS 1226 I-19805 144 (opened for signing 9 June 1977, entered into force 21 May 1980).

International Convention on Mutual Administrative Assistance in Customs Matters (Johannesburg Convention) (opened for signing 27 June 2003) (deposited at the WCO, no document number, retrieved from www.wcoomd.org).

International Convention on the Simplification and Harmonisation of Customs Procedures (as amended) (The Revised Kyoto Convention) (opened for signing 6 June 1999, entered into force 3 February 2006) (deposited at the WCO, no document number, retrieved from www.wcoomd.org).

International Convention on the Simplification and Harmonisation of Customs Procedures (The Kyoto Convention) (1974) (deposited at the WCO, no document number, retrieved from www.wcoomd.org).

International Covenant on Civil and Political Rights GA Res 2200A, A/RES/21/2200 (1966) (ICCPR).

New Zealand – Hong Kong, China Closer Economic Partnership Agreement UNTS 2479 I-48534 (2010).

Optional Protocol to the Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment A/RES/57/199 (opened for signing 18 December 2002, entered into force 22 June 2006).

Protocol 2 for Mutual Administrative Assistance in Customs Matters, European Union – Madagascar OJ L111/1161 (2012).

Protocol 2 for Mutual Administrative Assistance in Customs Matters, European Union – Mauritius OJ L111/1161 (2012).

Protocol 2 for Mutual Administrative Assistance in Customs Matters, European Union – Seychelles OJ L111/1161 (2012).

Protocol 2 for Mutual Administrative Assistance in Customs Matters, European Union – Zimbabwe OJ L111/1161 (2012).

Russian Federation and Belarus Customs Union UNTS 2212 I-39319 63 (2004).

Stabilisation and Association Agreement, European Union – Albania OJ L107/165 (2009).

Trade Agreement, European Union – Denmark and Faroe Islands OJ L53/1 (1996).

Vienna Convention on the Law of Treaties 1155 UNTS 331 (1969).

## *Cases*

*American Civil Liberties Union v Clapper* 785 F 3d 787 (2d Cir 2015).

*Attorney-General v Kim Dotcom* [2014] NZCA 19.

*Attorney-General v Ahmed Zaoui* SC CIV 19/2004 [2005] NZSC 38.

*Baird v State Bar* 401 US 1 (1971).

*Bathurst City Council v Saban* [1985] 2 NSWLR 704.

*Bathurst Developments Ltd v New Zealand Customs Service* [1998] DCR 300.

*Belhadj v the Security Service, SIS, GCHQ, Home Office and FCO* [2015] IPT/13/132-9/H.

*Binyam Mohamed v Secretary of State for Foreign and Commonwealth Affairs* [2008] EWHC 2048, 2100, 2519, 2549, 2973 (Admin) [2009] EWHC 152 (Admin) [2010] EWCA Civ 65.

*Brown v Attorney-General* [2006] DCR 630.

*Bykov v Russia* (4378/02) Grand Chamber, ECHR 10 March 2009.

*C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672.

*Campbell v Mirror Group Newspapers Limited* [2004] UKHL 22, [2004] 2 AC 457, [2 WLR 1232, [2004] 2 All ER 995 (HL).

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Secretary of State for the Home Department v Post-och telestyrelsen and Others* [2016] ECR 970.

*Council of Civil Service Unions and Others v Minister for the Civil Service* [1983] UKHL 6, [1985] AC 374, [1984] 3 WLR 1174, [1985] ICR 14, [1984] 3 All ER 935, [1985] IRLR 28.

*Crimmins v Stevedoring Industry Finance Committee* [1999] HCA 59, [1999] 200 CLR 1.

*DoJ v Reporters Committee for Freedom of the Press* 489 US 749 (1989).

*Dotcom v Attorney-General* [2012] NZHC 1494, [2012] 3 NZLR 115.

*Dotcom v Attorney-General* [2013] NZHC 1269.

*Dotcom v Attorney-General* [2014] NZSC 199.

*Dulcie Holdings Ltd v New Zealand Customs Service* [1997] DCR 1077.

*El-Masri v Former Yugoslav Republic of Macedonia* [2012] ECHR 2067, (2013) 57 EHRR 25, 57 EHRR 25, 34 BHRC 313.

*Entick v Carrington* (1765) 19 St Tr 1030, (1765) 19 St Tr 1029, [1765] EWHC KB J98, [1558-1774] All ER Rep 41, 95 ER 807.

*Garrett v Attorney-General* [1997] 2 NZLR 332 (CA).

*Hamed v R* [2011] NZSC 101.

*Hosking v Runting* [2004] NZCA 34, [2005] 1 NZLR 1.2004] NZCA 34.

*Hunt v Central Intelligence Agency* 981 F 2d 1116 (1992).

*Kennedy v Ireland* [1987] IR 587.

*Khan v United Kingdom* [2000] ECHR 194, (2000) 31 EHRR 1016, [2000] ECHR 195, (2001) 31 EHRR 45.

*Klayman v Obama* 957 F Supp 2d 1 (DC Cir 2015).

*Liberty (The National Council of Civil Liberties) and Others v the Secretary of State for Foreign and Commonwealth Affairs and Others* [2015] IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH.

*Liversidge v Anderson* [1941] UKHL 1, [1941] 3 All ER 338, [1942] AC 206.

*Malone v United Kingdom* [1985] ECHR 5, (1984) 7 EHRR 14, [1984] ECHR 10.

*McCormick v England* 494 SE 2d 431, 432 (SC Ct App 1997).

*Murray v Express Newspapers Plc* [2008] EWCA Civ 446, [2009] Ch 481,[2008] 3 WLR 1360, [2008] ECDR 12, [2008] EMLR 12 [2008] 2 FLR 599, [2008] 3 FCR 661, [2008] HRLR 33, [2008] UKHRR 736, [2008] Fam Law 732 (CA).

*Nakkuda Ali v M F de S Jayaratne* 66 TLR (Pt 2) 214, (1950) 10 CR 421, [1951] AC 66, [1950] UKPC 17.

Opinion 1/15 of the Court (Grand Chamber) [2017] ECR 592.

*Prince Albert v Strange* [1849] EWHC Ch J20, (1849) 18 LJ Ch 120, (1849) 1 Mac & G 25, 41 ER 1171.

*R v Hawea* [2009] NZCA 127.

*R v McGaughey* [2007] NZCA 411.

*R v Shaheed* [2002] 2 NZLR 377 (CA).

*R v Williams* [2007] NZCA 52.

*Rhodes v OPO* [2015] UKSC 32.

*Simpson v Attorney-General* [Baigent's Case] [1994] 3 NZLR 667 (CA).

*Snepp v United States* 444 US 507 (1980).

*Sporrong and Lonroth v Sweden* (1983) 5 EHRR 35.

*Three Rivers District Council v Governor and Company of the Bank of England* [2001] UKHL 16, (2001) 3 LGLR 36, [2001] 2 All ER 513, [2003] 2 AC 1, [2001] Lloyds Rep Bank 125, [2001] Lloyd's Rep Bank 125.

*Von Hannover v Germany* [2004] ECHR] 294.

*Wainwright v Home Office* [2003] UKHL 53, [2004] UKHRR 154, [2004] 2 AC 406, [2003] 4 All ER 969, 15 BHRC 387, [2003] 3 WLR 1137.

*Wilkinson v Downton* [1897] 2 QB 57, [1897] EWHC 1 (QB).

*Zaoui v Attorney-General* [2005] NZSC 38, [2005] 1 NZLR 666, [2005] 1 NZLR 690, [2006] 1 NZLR 289.

## *Legislation*

***Argentina***

Data Protection Act 2000.

***Australia***

Inspector-General of Intelligence and Security Act 1986.

Intelligence Services Act 2001 (ASIS Act).

Privacy Act 1988.

Privacy Amendment (Enhancing Privacy Protection) Act 2012.

***Canada***

Canadian Security Intelligence Service Act 1985 (Canada SIS Act).

Personal Information Protection and Electronic Documents Act 2000.

Privacy Act 1983.

***China, People's Republic of***

Criminal Law Amendment (9) (刑法修正案（九）条文) 2015.

Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Internet Information (Adopted at the 30th Meeting of the Standing Committee

of the National People's Congress on December 28, 2012) (全国人民代表大会常务委员会关于加强网络信息保护的决定 (2012年12月28日第十一届全国人民代表大会常务委员会第三十次会议通过).

***Hong Kong***

Personal Data (Privacy) Ordinance 2013.

***Italy***

Constitution (Costituzione Della Repubblica Italiana) 1947.

***Japan***

Amended Act on the Protection of Personal Information 2015.

Personal Information Protection Act 2003.

***Korea, South***

Public Agency Data Protection Act 1995.

***New Zealand***

Crimes Act 1961.

Crimes of Torture Act 1989.

Criminal Records Act 2004 (Clean Slate Act).

Customs and Excise Act 1996.

Customs and Excise Amendment Act 2004.

Double Tax Agreements (United States of America—FATCA) Order 2014/209.

Evidence Act 2006.

Government Communications Security Bureau Act 2003 (GCSB Act).

Immigration (Carriers' Infringement Offences, Fees and Forms) Regulations 2012 SR 2012/106.

Immigration Act 1987.

Immigration Act 2009.

Immigration Amendment Act 1999.

Inspector-General of Intelligence and Security Act 1996.

Intelligence and Security Act 2017.

Mutual Assistance in Criminal Matters Act 1992.

New Zealand Bill of Rights Act 1990.

New Zealand Security Intelligence Service Act 1969 (NZSIS Act).

Official Information Act 1982.

Ombudsmen Act 1975.

Privacy (Information Sharing Agreement Between Inland Revenue and Internal Affairs) Order 2014 LI 2014/223.

Privacy Act 1993.

Privacy Amendment Act 2013.

Protected Disclosures Act 2000.

***Russian Federation***

Law of the Russian Federation on Information, Informatization, and Information Protection 1995 (Russian Federation).

***Sri Lanka (formerly Ceylon)***

Defence (Control of Textiles) Regulations 1945.

***United Kingdom***

Data Protection Act 1984.

Intelligence Services Act 1994 (MI5 and MI6 Act).

Privacy and Electronic Communications (EC Directive) Regulations 2003.

Terrorism Prevention and Investigation Measures Act 2011.

***United States***

5 USC § 552 s (b)(7)(E).

50 USC § 1802.

82 FR 8497 Presidential Memorandum Regarding Withdrawal of the United States from the Trans-Pacific Partnership Negotiations and Agreement, 23 January 2017.

115 Stat 224 Authorisation for the Use of Military Force.

115 Stat 272 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001 (The PATRIOT Act).

118 Stat 3638 Intelligence Reform and Terrorism Prevention Act 2004.

Economic Espionage Act 18 USC § 1831-1839.

Espionage Act 18 USC § 792.

Executive Order 13492 Review and Disposition of Individuals Detained at the Guantanamo Bay Naval Base and Close of Detention Facilities 74 FR 4897, 27 January 2009.

Executive Order 13493 Review of Detention Policy Options 74 FR 4901, 27 January 27 2009.

Fourth Amendment to the United States Constitution (1792).

USA Freedom Act 50 USC § 1862.

## *Other International Material*

*Authorised Economic Operators: Guidelines* TAXUD/B2/047/2011–Rev.5 (2014).

*Daily Edition: Daily Digest/Senate Committee Meetings* 115th Congress, 1st Session Issue: Vol 163, No 177 (1 November 2017).

*e-Customs Progress Report* TAXUD.A.3(2017)3921405 (2016).

*Human Rights Council: Report of the Working Group on the Universal Periodic Review - New Zealand* A/HRC/26/3/Add 1 (2014).

*Intelligence Activities and the Rights of Americans: Book II - Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities* [1976] 94th Congress 2nd Session, S Rept 90-755.

*Joint WCO/UNCITRAL Working Group on Model Legal Guidelines for Implementation of Integrated Border Management* PC0197E (2007).

*Paperless Trade in International Supply Chains: Enhancing Efficiency and Security* ECE/TRADE/351 (2008).

*Recommendation No. 33: Recommendation and Guidelines on establishing a Single Window* ECE/TRADE/352 (2005).

*Recommendation No. 35: Establishing a legal framework for international trade Single Window* ECE/TRADE/401 (2010).

*Recommendation No. 36: Single Window Interoperability* ECE/TRADE/C/CEFACT/2017/6.

*Security Council Resolition on Foreign Terrorist Fighters* S/RES/2178 (2014).

*Security Council Resolution on Measures to Guarantee the Safety and Protection of the Palestinian Civilians in Territories Occupied by Israel* S/RES/904 (1994).

*Security Council Resolution on the Responsibility to Protect Civilians* S/RES/1265 (1999).

*Security Council Resolution Reaffirming the Responsibility to Protect Civilians* S/RES/1674 (2006).

*Security Council Resolution Reaffirming the Responsibility to Protect Civilians* S/RES/1296 (2000).

*The Situation in Libya* S/RES/1973 (2011).

*Universal Declaration of Human Rights* GA Res 217A, A/RES/3/217 A (III) (1948) (UDHR).

*The Single Window Concept: Enhancing the Efficient Exchange of Information between Trade and Government* ECE/TRADE/324 (2003).

## *Books and Sections in Books*

Ruwantissa Abeyratne *Strategic Issues in Air Transport: Legal, Economic and Technical Aspects* (Springer Science and Business Media, Montreal, 2012).

Josef L Altholz, Damian McElrath and James C Holland (eds) *The Correspondence of Lord Acton and Richard Simpson Volume II* (Cambridge University Press, London, 1978).

Malcolm Anderson *Policing the World : Interpol and the Politics of International Police Co-operation* (Clarendon Press, New York, 1989).

David Anderson QC *A Question of Trust: Report of the Investigatory Powers Review* (Her Majesty's Stationery Office, London, 2015).

Ross J Anderson *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed, Wiley, Indianapolis, IN, 2008).

Peter Andreas and Ethan Nadelmann *Policing the Globe: Criminalization and Crime Control in International Relations* (Oxford University Press, New York, 2006).

APEC Sub-Committee on Customs Procedures *Working Towards the Implementation of Single Window within APEC Economies: Single Window Development Report* (Australian Customs Service, Canberra, 2007).

Marc Augé *A Sense of the Other* (Stanford University Press, Palo Alto, 1998).

John Barrell *The Spirit of Despotism: Invasions of Privacy in the 1790s* (Oxford University Press, Oxford, 2006).

Alison Bashford *Medicine at the Border: Disease, Globalisation and Security, 1850 to the Present* (Palgrave Macmillan, Basingstoke, 2006).

Tom L Beauchamp and James F Childress *Principles of Biomedical Ethics* (5th ed, Oxford University Press, New York, 2001).

Larry W Beeferman *Images of the Citizen and the State: Resolving the Paradox of Public and Private Power in Constitutional Law* (University Press of America, Lanham, MA, 1996).

Emma Bell *Soft Power and Freedom Under the Coalition: State-Corporate Power and the Threat to Democracy* (Palgrave MacMillan, Basingstoke, 2015).

Richard Bellamy (ed) *Beccaria: On Crimes and Punishments and Other Writings* (Cambridge University Press, Cambridge UK, 1995).

Hossein Bidgoli (ed) *Global Perspectives in Information Security* (Wiley & Sons, New Jersey, 2004).

Peter Bondanella and Mark Musa (eds) *The Portable Machiavelli* (Penguin, Middlesex, 1979).

Els De Busser *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities* (Maklu, Antwerp, 2009).

Cambridge University Press *Cambridge Business English Dictionary* (Cambridge University Press, Cambridge UK, 2011).

Emelios Christodoulidis and StephenTierney (eds) *Public Law and Politics: the Scope and Limits of Constitutionalism* (Ashgate, Aldershot, 2008).

Michael P Colaresi *Democracy Declassified: the Secrecy Dilemma in National Security* (Oxford University Press, New York, 2014).

Joel Colon-Rios *Weak Constitutionalism: Democratic Legitimacy and the Question of Constituent Power* (Rutledge, Abingdon, 2012).

Russel Cropanzano and Alicia Grandley "If Politics is a Game, Then What are the Rules?: Three Suggestions for Ethical Management" in Marshall Schminke (ed) *Managerial Ethics: Moral Management of People and Processes* (Lawrence Erlbaum & Associates, Mahwah NJ, 1998) 133.

Francis Mading Deng, Sadikiel Kimaro, Terrence Lyons and others *Sovereignty as Responsibility: Conflict Management in Africa* (The Brookings Institution, Washington DC, 1996).

George Duncan "Exploring the Tension Between Privacy and the Social Benefits of Government Databases" in Peter Shane, John Podesta and Richard Leone (eds) *A little knowledge: privacy, security and public information after September 11* (Century Foundation Press, New York, 2004) 71.

European Commission Customs Policy Committee *A Guide to Risk Analysis and Customs Controls* (Office for Official Publications of the European Communities, Luxembourg, 1999).

David Feldman "The Politics and People of Entick v Carrington" in Adam Tomkins and Paul Scott (eds) *Entick v Carrington: 250 Years of the Rule of Law* (Hart Publishing, Oxford, 2015) 5.

John G Fleming *The Law of Torts* (The Law Book Company, Agincourt (Ontario), 1992).

Jane Fountain *Building the Virtual State: Information Technology and Institutional Change* (Brookings Institution Press, Washington DC, 2001).

Charles Fried *An Anatomy of Values* (Harvard University Press, Cambridge MA, 1970).

Lawrence M Friedman *The Human Rights Culture: A Study in History and Context* (Quid Pro Books, New Orleans, 2011).

Edward Gibbon (originally published 1776) *The History of the Decline and Fall of the Roman Empire: A New Edition, In One Volume* (T Cadell, London, 1837).

Sir Peter Gibson *The Report of the Detainee Inquiry* (The Stationery Office Limited, London, 2013).

Peter Gill *Policing Politics: Security Intelligence and the Liberal Democratic State* (Frank Cass, London, 1994).

Andrew Goldsmith and James Sheptycki *Crafting Transnational Policing: Police Capacity-Building and Global Policing Reform* (Hart Publishing, Oxford, 2007).

Benjamin Goold and Daniel Neyland *New Directions in Surveillance Privacy* (Routledge, London, 2013).

Glenn Greenwald *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books, New York, 2014).

Julian Grenfell and Richard P Wright *The EU/US Passenger Name Record (PNR) Agreement: Report with Evidence, 21st Report of Session 2006-07* (Stationery Office, London, 2007).

Jurgen Haacke *ASEAN's Diplomatic and Security Culture: Origins, Development and Prospects* (Routledge, Birmingham, 2013).

Bernard E Harcourt *Exposed: Desire and Disobedience in the Digital Age* (Harvard University Press, Cambridge MA, 2015).

Carol Harlow *State Liability: Tort Law and Beyond* (Oxford University Press, Oxford, 2004).

Neil Hicks "The Impact of Counter Terror on the Promotion and Protection of Human Rights: A Global Perspective" in Richard Ashby Wilson *Human Rights in the War on Terror* (Cambridge University Press, Cambridge UK, 2006).

John Eldred Howard (ed) *Napoleon Bonaparte: Letters and Documents of Napoleon, Volume I: the Rise to Power* (The Cresset Press, London, 1961).

Deborah Hurley "Taking the Long Way Home: the Human Right of Privacy" in Marc Rotenberg, Julia Horowitz and Jeramie Scott *Privacy in the Modern Age: the Search for Solutions* (The New Press, New York, 2015) 70.

Loch K Johnson *A Season of Inquiry: the Senate Intelligence Investigations* (The University Press of Kentucky, Lexington, 1985).

Sarah Joseph and Adam McBeth (eds) *Research Handbook on International Human Rights Law* (Edward Elgar Publishing, Cheltenham, 2010).

Jeffrey Kahn *Mrs. Shipley's Ghost: the Right to Travel and Terrorist Watchlists* (University of Michigan Press, Ann Arbor, 2013).

Mary Kaldor "Human Security" in Mary Kaldor and Iavor Rangelov (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 85.

Immanuel Kant, James W Ellington (translator) *Grounding for the Metaphysics of Morals* (3rd ed, Hackett Publishing, Indianapolis, 1993).

Peter Kaye *An Explanatory Guide to the English Law of Torts* (Barry Rose Law Publishers, Chichester, 1996).

Thomas H Kean, Lee H Hamilton, Richard Ben-Veniste Fred F Fielding and Others *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Government Printing Office, Washington DC, 2004).

Sesha Kethinini (ed) *Comparative and International Policing, Justice, and Transnational Crime* (Carolina Academic Press, Durham NC, 2010).

Rob Kitchin *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences* (Sage Publications, London, 2014).

Vicesimus Knox *The Spirit of Despotism* (2nd ed, William Hone, London, 1821).

Andrew Ladley and Nicci Simmons *Conceptualising the Border and Customs in the 21st Century - or How to Outfox the Future* (Institute of Policy Studies, Wellington, 2007).

Klaus von Lampe "The Practice of Transnational Organized Crime" in Felia Allum and Stan Gilmour (eds) *Routledge Handbook of Transnational Organized Crime* (Routledge, Abingdon, 2012).

Ian Leigh "Accountability of Security and Intelligence in the United Kingdom" in Hans Born, Lock K Johnson and Ian Leigh *Who's Watching the Spies: Establishing Intelligence Service Accountability* (Potomac Books, Dulles VA, 2005) 79.

C L Lim, Deborah K Elms and Patrick Low *The Trans-Pacific Partnership: A Quest for a Twenty-first Century Trade Agreement* (Cambridge University Press, New York, 2012).

Ian Loader and Neil Walker *Civilizing Security* (Cambridge University Press, Cambridge, 2007).

David Luban "Eight Fallacies about Liberty and Security" in Richard Ashby Wilson *Human Rights in the War on Terror* (Cambridge University Press, Cambridge UK, 2006) 242.

David Lyon *Surveillance after Snowden* (Polity, Cambridge, UK, 2015).

Niccolò di Bernardo dei Machiavelli "The Prince" in Peter and Mark Musa (eds) Bondanella *The Portable Machiavelli* (Penguin, Middlesex, 1979) 77.

Justin Malbon and Bernard Bishop *Australian Export* (2nd ed, Cambridge University Press, Melbourne VIC, 2014).

Susan Maret (ed) *Government Secrecy* (Emerald Group Publishing, Bingley, UK, 2011).

Colleen McCue *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis* (2nd ed, Butterworth-Hienemann, Oxford, 2015).

Don McDowell *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users* (Scarecrow Press, Plymouth, 2008).

Simon McKay *Covert Policing: Law and Practice* (Oxford University Press, Oxford, 2011).

T Lambert Mears (translator) *The Institutes of Gaius and Justinian, the Twelve Tables, and the CXVIIIth and CXXVIIth Novels* (Stevens and Sons, London, 1882).

Peter Mento *C-TPAT and ISA, Understanding the Effectiveness of Trade Partnerships for Customs Enforcement* (Lulu Press, Raleigh NC 2004).

Gorazd Mesko and Robert Furman "Police and Prosecutorial Cooperation in Responding to Transnational Crime" in Philip L Reichel and Jay S Albanese (eds) *Handbook of Transnational Crime and Justice* (Sage Publications, Thousand Oaks CA, 2014) 323.

C William Michaels *No Greater Threat: America After September 11 and the Rise of a National Security State* (Algora Publishing, New York, 2007).

Breon Mitchell (translator) *The Trial/Franz Kafka: a New Translation Based on the Restored Text* (Schocken, New York, 1998).

Barrington Moore *Privacy: Studies in Social and Cultural History* (ME Sharpe, Armonk NY, 1984).

David Mutimer "Security and Social Critique" in Mary Kaldor and Iavor Rangelow (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 31.

New Zealand Customs Service *Annual Report 2015/16* (New Zealand Customs Service, Wellington, 2016).

New Zealand Security Intelligence Service *New Zealand Government Security Classification System* (NZSIS, Wellington, 2017).

New Zealand State Services Commission and The Treasury *Performance Measurement: Advice and Examples on How to Develop Effective Frameworks* (Wellington, 2008).

Patrick O'Callaghan *Refining Privacy in Tort Law* (Springer Science & Business Media, Newcastle UK, 2012).

Office of the United Nation's High Commissioner for Human Rights *Human Rights and Law Enforcement: A Trainer's Guide on Human Rights for the Police, Issue 5, Part 2* (United Nations, Geneva, 2002).

George Orwell *Nineteen Eighty-Four* (Everyman's Library, London, 1992).

Frank Pasquale "Privacy, Autonomy and Internet Platforms" in Marc Rotenburg, Julia Horowitz and Jeramie Scott *Privacy in the Modern Age: the Search for Solutions* (The New Press, New York, 2015) 165.

Stephen Penk "Common Law Privacy Protection in other Jurisdictions" in Stephen Penk, Rosemary Tobin, Khylee Quince, Bill Hodge, Donna Maree Cross, Warren J Brookbanks, Natalya King, Pauline Tapp, Hon Judge David Harvey Privacy Law in New Zealand (2nd ed, Brookers, Wellington, 2016) 113.

Daniel Philpott "Protection of Nations and Minorities: the Road to Versailles" in Sohail H Hashimi (ed) *State Sovereignty: Change and Persistence in International Relations* (Pennsylvania State Press, Pennsylvannia, 2010) 34.

Russ Porter "Intelligence-led Policing and Public Trust" in Jerry Ratcliffe, Intelligence-led Policing (Willan, Devon UK, 2008) 222.

Paul J Quirk and Joseph Hinchcliffe "The Rising Hegemony of Mass Opinion" in David Brian Robertson (ed) *Loss of Confidence: Politics and Policy in the 1970s* (Pennsylvannia State Press, University Park PA, 2010) 19.

Jerry Ratcliffe *Intelligence-led Policing* (Willan Publishing, Devon UK, 2008).

Priscilla Regan *Legislating Privacy: Technology, Social Values and Public Policy* (2nd ed, University of North Carolina Press, Chapel Hill NC, 2009).

Darius Rejali *Torture and Democracy* (Princeton University Press, New Jersey, 2007).

Fiona Robinson *The Ethics of Care: A Feminist Approach to Human Security* (Temple University Press, Philadelphia PA, 2011).

Frederick Rosen *Classical Utilitarianism From Hume to Mill* (Routledge, London, 2003).

Marc Rotenberg, Julie Horwitz and Jeramie Scott *Privacy in the Modern Age: the Search for Solutions* (The New Press, New York, 2015).

James Rule *Privacy in Peril: How we are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Oxford University Press, New York, 2007).

Philip N Rumney *Torturing Terrorists: Exploring the Limits of Law, Human Rights and Academic Freedom* (Routledge, Abingdon, Oxon, 2014).

Carl Schmitt, Ellen Kennedy (translator) *The Crisis of Parliamentary Democracy (1923)* (MIT Press, Cambridge MA, 1985).

Carl Schmitt, George Schwab (translator) *Political Theology: Four Chapters on the Concept of Sovereignty* (University of Chicago Press, Chicago, 2005).

Carl Schmitt, Jeffrey Seitzer (translator) *Constitutional Theory (1928)* (Duke University Press, Durham NC, 2008).

Christoph H Schreuer *The ICSID Convention: A Commentary* (Cambridge University Press, Cambridge UK, 2001).

Frederick A Schwarz *Democracy in the Dark: the Seduction of Government Secrecy* (The New Press, New York, 2015).

Sabine Selchow "Security Policy and Global Risks" in Mary Kaldor and Iavor Rangelov (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 68.

Senate Select Committee on Intelligence *Unclassified: Committee Study of the Central Intelligence Agency's Detention and Interrogation Program* (United States Senate, Washington DC, 13 December 2012).

James Sheptycki "The Drug War: Learning from the Paradigm of Transnational Policing" in James Sheptycki (ed) *Issues in Transnational Policing* (Routledge, London, 2000) 201.

Marie Shroff *Necessary and Desirable: Privacy Act 1993 Review Highlights* (Privacy Commissioner, Wellington, 1998).

Robin Simcox *Surveillance after Snowden: Effective Espionage in an Age of Transparency* (The Henry Jackson Society, London, 2015).

Paul Smith (ed) *Terrorism and Violence in Southeast Asia: Transnational Challenges to States and Regional Stability* (East Gate, New York, 2005).

Daniel J Solove *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 2006).

Jenny Steele *Tort Law: Text, Cases and Materials* (2nd ed, Oxford University Press, Oxford, 2010).

Ekaterina Stepanova "Terrorism and Antiterrorism" in Mary Kaldor and Iavor Rangelov (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 126.

Kati Suominen *Fueling the Online Trade Revolution: A New Customs Security Framework to Secure and Facilitate Small Business E-Commerce* (Rowman & Littlefield, Lanham MD, 2015).

George Sutherland *Constitutional Power and World Affairs* (Columbia University Press, New York, 1918).

Athan Theoharis *The Quest for Absolute Security: the Failed Relations Among US Intelligence Agencies* (Ivan R Dee, Chicago, 2007).

Jeffrey L Thomas *Scapegoating Islam: Intolerance, Security, and the American Muslim* (ABC-CLIO, Santa Barbara, 2015).

Stephen Todd, Cynthia Hawes, Bill Atkin, Ursula Cheer and John Burrows *The Law of Torts in New Zealand* (6th ed, Thomson Reuters, Wellington, 2013).

Catherine Truel *A Short Guide to Customs Risk* (Gower, London, 2010).

United Kingdom Chief of the General Staff *Operation Banner: an Analysis of Military Operations and Northern Ireland (Army Code 71842)* (Ministry of Defence, London, July 2006).

United Kingdom Government *Government Security Classifications April 2014* (Her Majesty's Stationery Office, London, 2013).

United Kingdom Government *National Security Strategy and Strategic Defence and Security Review 2015* (Her Majesty's Stationery Office, London, 2015).

United Kingdom Government *National Security Strategy and Strategic Defence and Security Review 2015: First Annual Report 2016* (Her Majesty's Stationery Office, London, 2016).

United Kingdom Government *HM Government Response to the House of Lords Select Committee on the Constitution 4th Report of Session 2010-2012: Justice and Security Bill [HL]: Norwich Pharmacal Jurisdiction (CM 8460)* (Her Majesty's Stationery Office, London, 2012).

United Kingdom Intelligence and Security Committee *Annual Report 1997-1998* (The Stationery Office, London, 1998).

United Kingdom Joint Committee on Human Rights *Allegations of UK Complicity in Torture: Twenty–third Report of Session 2008–09* (The Stationery Office Limited, London, 2009).

United Kingdom National Audit Office *HM Revenue & Customs' Transformation Programme: Report* (The Stationary Office, London, 2008).

United States General Accounting Office *Money Laundering and Currency: Smuggling: An Assessment* (DIANE Publishing Company, Washington DC, 1994).

United States President's Council of Advisors on Science and Technology *Report to the President - Big Data and Privacy: a Technological Perspective* (Office of the President of the United States, Washington DC, May 2014).

Willemijn Verkoren and Mathijs van Leeuwen "Civil Society in Fragile Contexts" in Mary Kaldor and Iavor Rangelov (eds) *The Handbook of Global Security Policy* (Wiley Blackwell, Chichester, 2014) 463.

David Vincent *I Hope I Don't Intrude: Privacy and its Dilemmas in Nineteenth-Century Britain* (Oxford University Press, Oxford, 2015).

Clive Walker and Andrew Staniforth "The Amplification and Melding of Counter-Terrorism Agencies: From Security Services to Police and back again" in Aniceto Masferrer and Clive Walker *Counter – Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State* (Edward Elgar, Cheltenham, 2013) 293.

Clive Walker and Javaid Rehman "'Prevent' Responses to Jihadi Extremism" in Victor V RamRaj, Michael Hor, Kent Roach, and George Williams *Global Anti-Terrorism Law and Policy* (2nd ed, Cambridge University Press, Cambridge UK, 2012) 242.

Clive Walker *Terrorism and the Law* (Oxford University Press, Oxford, 2011).

Neil Walker "The Pattern of Transnational Policing" in Tim Newburn (ed) *Handbook of Policing* (Willan Publishing, Abingdon, 2008) 119.

Michele Wilson "Community in the Abstract: A Political and Ethical Dilemma" in David Holmes (ed) *Virtual Politics: Identity and Community in Cyberspace* (Sage Publications, London, 1997) 145.

Christopher Wolf and Marc Rotenberg "Envisioning Privacy in the World of Big Data" in Julia Horwitz and Jeramie Scott *Privacy in the Modern Age: the Search for Solutions* (The New Press, New York, 2015) 204.

World Customs Organisation and UNCTAD *Risk Management in Customs procedures* (UNCTAD, Geneva, 2008).

Luc De Wulf and Jose B Sokol *Customs Modernization Handbook* (World Bank, Washington DC, 2005).

## *Journal Articles*

Irwin Altman "Privacy Regulation: Culturally Universal or Culturally Specific?" (1977) 33(3) Journal of Social Issues 66-84.

Irwin Altman "Privacy: A Conceptual Analysis" (1976) 8(1) Environment and Behavior 7-30.

Maurice Atkinson and Valerie Maxwell "Driving Performance in a Multi-Agency Partnership using Outcome Measures: A Case Study" (2007) 11(2) Measuring Business Excellence 12-22.

J Samuel Barkin and Bruce Cronin "The State and the Nation: Changing Norms and the Rules of Sovereignty in International Relations" (1994) 48(1) International Organisation 107-130.

Emily Berman "Quasi-Constitutional Protections and Government Surveillance" (2016) 3 BYU L Rev 771-836.

Seniz Bigli "Intelligence Cooperation in the European Union: An Impossible Dream?" (January 2016) 5(1) All Azimuth 57-67.

Ben Bowling "Transnational Policing: the Globalization Thesis, a Typology and a Research Agenda" (2009) 3 (2) Policing: A Journal of Policy and Practice 149-160.

Chris Clough "Quid Pro Quo: the Challenges of International Strategic Intelligence Cooperation" (2004) 17(4) International Journal of Intelligence and CounterIntelligence 601-613.

Joel Colon-Rios "Five Conceptions of Constituent Power" (2014) 130 LQR 306.

Simon Consedine "R v Shaheed: the First Twenty Months" (2004) 10(1) Canterbury L Rev 77-104.

Karine Cote-Boucher "The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada's Smart Border" (2008) 5(2) Surveillance and Society 142-165.

Melissa De Zwart, Sal Humphries and Beatrix Van Dissel "Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK" (2014) 37(2) UNSWLJ 713-747.

Natasha Stott Despoja "A Brief Look at the History of Privacy" (2007) 79(3) Australian Quarterly.

Martyn Dunne "New Zealand Customs Service: Changes over the Last Decade and into the Future" (2007) 1(1) World Customs Journal 41-47.

Gareth Evans and Mohamed Sahnoun "The Responsibility to Protect" (2002) 81(6) Foreign Affairs 99-110.

Helen Fessenden "The Limits of Intelligence Reform" (2005) 84(6) Foreign Affairs 106-120.

Charles Fried "Privacy" (1968) 77(3) Yale LJ 475-493.

J William Fulbright "The High Cost of Secrecy" (1971) 39(9) The Progressive American Review of Public Administration 16-21.

Francesca Galli, Valsamis Mitsilegas and Clive Walker "Terrorism investigations and prosecutions in comparative law" (2016) 20(5) The International Journal of Human Rights 593-600.

Ruth E Gavison "Privacy and the Limits of the Law" (1980) 89(3) Yale LJ 421-471.

Robert Gellman "Public Records, Public Policy, and Privacy" (1999) 26(1) Human Rights 7-9.

Andrew J Glass "Congressional Report/Legislative Reform Effort Builds New Alliances Among House Members" (1970) 2 National Journal 1607–1614.

A M Gordon "Do Drug Offences Matter?" (1978) 2(6131) British Medical Journal 185-186.

Georg Dieter Gotschlich "The World Wide Developments of International Customs Law" (1998) 7 International Business LJ 947-956.

Graham Greenleaf "Global Data Privacy Laws 2015: 109 Countries with European Laws now in a Minority" (2015) 133 Privacy Laws & Business International Report 14-17.

CarrieLyn Donigan Guymon "International Legal Mechanisms for Combating Transnational Organized Crime: the Need for a Multilateral Convention" (2000) 18 1) Berk J Intl L 53-101.

Alice Hills "The possibility of transnational policing" 19(3) Policing and Society: An International Journal of Research and Policy 300-317.

Christopher Hoadley, Heng Xu, Joey J Lee and Mary Beth Rosson "Privacy as Information Access and Illusory Control: the case of the Facebook News Feed Privacy Outcry" (2010) 9 Electronic Commerce Research and Applications 50-60.

Andrew Hosking "Australian Customs Service: Working to Improve Facilitation of International Trade and the Security of the Supply Chain Within the Apec Region" (2012) 1(2) World Customs Journal 67-69.

Saskia Hufnagel "Cross-Border Police Co-operation: Traversing Domestic and International Frontiers" (2011) 35 Crim LJ 333-344.

Saskia Hufnagel "'The Fear of Insignificance': New Perspectives on Harmonising Police Cooperation in Europe and Australia" (2010) 6(2) Journal of Contemporary European Research 165-193.

Chris DI Hunt "New Zealand's New Privacy Tort in Comparative Perspective" (2013) 13(1) OUCLJ 157-166.

Lani Inverarity "Immigration Bill 2007: Special Advocates and the Right to be Heard" (2009) 40 VUWLR 471-506.

Emilia Iordache and Alina Vasilica Voiculet "Customs Risk Management in the European Union" (2007) 10(25) Romanian Economic Journal 55-71.

Christopher Kuner, Fred H Cate, Christopher Millard and Dan Jerker B Svantesson "The Challenge of 'Big Data' for Data Protection" (2012) 2(2) International Data Privacy Law 47-49.

Sir Stephen Lander "International Intelligence Cooperation: an Inside Perspective" (2004) 17(3) Cambridge Review of International Affairs 481.

David Lange "New Zealand's Security Policy" (Summer 1985) 63(5) Foreign Affairs 1009-1019.

Stephane Lefebvre "The Difficulties and Dilemmas of International Intelligence Cooperation" (2003) 16(4) International Journal of Intelligence and CounterIntelligence 527-542.

Ian Leigh "Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11" (2012) 27(5) Intelligence and National Security 722-738.

Adam D Moore "Privacy: Its Meaning and Value" (2003) 40(3) American Philosophical Quarterly 215-227.

Nicole Moreham "Beyond Information: Physical Privacy in English Law" (2014) 73(2) CLJ 350.

Nicole Moreham "Privacy in the Common Law: a Doctrinal and Theoretical Analysis" (2005) 121 LQR 628.

Daniel R Ortiz "Privacy, Autonomy and Consent" (1989) 12 Harv JL & Pub Pol'y 91-97.

W A Parent "Privacy, Morality and the law" (1983) 12 Philosophy and Public Affairs 269-288.

Robert G Patman and Laura Southgate "National Security and Surveillance: the Public Impact of the GCSB Amendment Bill and the Snowden Revelations in New Zealand" (2016) 31(6) Intelligence and National Security 871-887.

Jordan J Paust "Judicial Power to Determine the Rights and Status of Persons Detained Without Trial" (2003) 44 Harv Intl LJ 503-534.

John Pavolotsky "Privacy in the Age of Big Data" (2013) 69(1) The Business Lawyer 217-225.

Bernardo Perinan "The Origin of Privacy as a Legal value: A Reflection on Roman and English Law" (2012) 52(2) American Journal of Legal History 183-201.

Michael Plachta "Joint Investigation Teams - A New Form of International Cooperation" (2005) 13(2) European Journal of Crime, Criminal Law and Criminal Justice 284-302.

Mark Pythian "The British Experience with Intelligence Accountability" (2007) 22(1) Intelligence and Security 75-99.

Jerry Ratcliffe "Intelligence-led Policing" (2003) April(248) Trends and Issues in Crime and Criminal Justice 1.

Marta Raus, Barbara Flugge and Roman Boutellier "Electronic Customs Innovation: An Improvement of Governmental Infrastructures" (2009) 26 Government Information Quarterly 246-256.

George A Rennie "HM Customs and Excise IT and Intelligence Applications in Cross Border Control" (1998) (January) European Police and Government Security Technology 8-9.

Derek S Reveron "Old Allies, New Friends: Intelligence-Sharing in the War on Terror" (2006) 50(3) Orbis 453-468.

Leah Angela Robis "When Does Public Interest Justify Government Interference and Surveillance?" (2014) 15 Asia-Pacific Journal on Human Rights and the Law 203-218.

Ira S Rubinstein "Big Data: the End of Privacy or a New Beginning?" (2012) 3(2) International Data Privacy law 74-87.

Bill Ryan and Derek Gill "Managing for Joint Outcomes" (2008) 4(3) Policy Quarterly 39-43.

Christine Ryan and Peter Walsh "Collaboration of Public Sector Agencies: Reporting and Accountability Challenges" (2004) 17(7) International Journal of Public Sector Management 621-631.

Jennifer E Sims "Foreign Intelligence Liaison: Devils, Deals, and Details" (2006) 19 International Journal of Intelligence and CounterIntelligence 195-217.

Daniel J Solove "A Taxonomy of Privacy" (2006) 154 (3) Univ Penn Law Rev 477.

Daniel J Solove "Introduction: Privacy, Self Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880-1903.

Daniel J Solove "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53(6) Stan L Rev 1393-1462.

Patrick Stewart "Failed States and Global Security - Empirical Questions and Policy Dilemmas" (2007) 9(4) International Studies Review 644-662.

Tzvetan Todorov "Torture in the Algerian War" (2002) Summer (135/136) Sagalmuni 15.

Alan Toy "Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity" (2010) 24(2) NZULR 223-238.

Rachel Levinson Waldman "Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public" (2017) 66(3) Emory LJ 527-615.

Clive Walker "Clamping Down on Terrorism in the United Kingdom" (2006) 4(5) JICJ 1-15.

Clive Walker "Keeping Control of Terrorists without Losing Control of Constitutionalism" (2007) 59 Stan L Rev 1395-1463

Clive Walker "Investigative Journalism and Counter Terrorism Laws" (2017) 31(1) Notre Dame Journal of Law, Ethics and Public Policy 129-174.

Clive Walker "The Reshaping of Control Orders in the United Kingdom: Time for a Fairer Go, Australia" (2013) 37 Melb U L Rev 143-118.

Patrick F Walsh and Seumas Miller "Rethinking ‘Five Eyes’ Security Intelligence Collection Policies and Practice Post Snowden" (2016) 31(3) Intelligence and National Security 345-368.

Carol Warren and Barbara Laslett "Privacy and Secrecy: A Conceptual Comparison" (July 1977) 33(3) Journal of Social Issues 43-51.

Carsten Weerth "The Johannesburg Convention on Mutual Customs Assistance-is a new tool failing early?" (2016) 6(2) Customs Scientific Journal 35-46.

## *Conference Papers, Dissertations, Theses and other Works*

George Duncan "Exploring the Tension Between Privacy and the Social Benefits of Governmental Databases" (the Security, Technology, and Privacy: Shaping a 21st Century Public Information Policy conference, 24-25 April 2003, Washington DC).

Sian Elias CJ "Public Actors and Private Obligations – a Judicial Perspective" (the University of Hong Kong Obligations VII conference, University of Hong Kong Faculty of Law, 18 July 2014).

Diana Halloy "Human Rights During Argentina's Military Rule: the Politics of Forced Disappearances" (the 2nd Global International Studies Conference, Ljubljana, 2008).

Jack Hirshleifer "Privacy: its Origin, Function and Future" (the Economics and the Law of Privacy conference, University of Chicago, 30 November 1979).

John Joseph and Jeff Corkill "Information Evaluation: How one Group of Intelligence Analysts go about the Task " (the 4th Australian Security and Intelligence Conference, Edith Cowan University, 5 -7 December, 2011).

Trisha Rajput and Abhinayan Basu Bal "Chapter 16 - Creating Sustainable Global Supply Chains through Single Window and Paperless Trade Initiatives: Efforts of WTO and UNCITRAL in Perspective" (unpublished chapter in book Yves-Louis Sage (ed) "Harmonising Trade Law to enable Private Sector Regional Development", 7 November 2017).

Musa Tuzuner "The State-Level Determinants of the United States' International Intelligence Cooperation" (PhD Dissertation, Kent State University, 2009).

## European *Material*

Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on Mutual Assistance and Cooperation between Customs Administrations [1998] OJ C24/1.

Council Decision 2015/219/EU Replacing the Annex on the Sirene Manual for SIS II [2015] OJ L44/75.

Decision 2000/520/EC: Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions issued by the US Department of Commerce [2000] OJ L215/7.

Decision 2007/533/JHA on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II) [2007] OJ L205/63.

Decision 2008/333/EC Adopting the Sirene Manual and Other Measures for the Second Generation Schengen Information System (SIS II) [2008] OJ L123/1.

Decision 2008/334/JHA Adopting the Sirene Manual and Other Measures for the Second Generation Schengen Information System (SIS II) [2008] OJ L123/39.

Decision 2013/115/EU on the Sirene Manual and Other Measures for the Second Generation Schengen Information System (SIS II) [2013] OJ L71/1.

Decision Bringing Into Force the Convention Implementing the Schengen Agreement of 19 June 1990 [2000] OJ L239/19.

Decision on the Adequate Protection of Personal Data by New Zealand [2013] OJ L28/12.

Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31.

Directive 96/9/EC of the European Parliament and of the Council on the Legal Protection of Databases [1996] OJ L077.

Directive 2002/58/EC on Privacy in the Electronic Communications Sector [2002] OJ L201/37.

Directive 2016/681/EU on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132.

Electronic Customs Multi-Annual Strategic Plan: 2008 Yearly Revision [2008] TAXUD/477/2004 - Rev 9 – EN.

European Commission for Democracy through Law (Venice Commission) Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies [2013] CDL-AD(2015)006.

Regulation 515/97 On Mutual Assistance between the Administrative Authorities of the Member States and Cooperation between the latter and the Commission to ensure the Correct Application of the Law on Customs and Agricultural Matters OJ L82/1.

Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53.

Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Records to the United States Department of Homeland Security [2013] COM(2013) 844.

## *Newspapers and Magazines*

Editorial "A New Age of Espionage; Intelligence and Democracy" *The Economist* (online edition, London, 1 August 2015).

Kofi Anan "Two Concepts of Sovereignty" *The Economist* (online edition, London, 18 September 1999).

Marjorie Arons-Barron "Secrecy tips the case of the Trans-Pacific Partnership" *Milford Daily News* (online edition, Milford MA, 5 June 2015).

Chris Barton "Dilemma of the life-saving cards" *New Zealand Herald* (online edition, Auckland, 8 May 2009).

Owen Bowcott "'Five Eyes' Surveillance Pact Should be Published, Strasbourg Court Told" *The Guardian* (online edition, London, 9 September 2014).

Susan Davis "Senate Panel Approves 'Fast Track' Trade Bill" *USA Today* (online edition, McLean VA, 22 April 2015).

Editorial “Spies, Torture and Terrorism: the Dark Pursuit of Truth” *The Economist* (online edition, London, 30 July 2009).

Paul Farrell "History of 5 Eyes – Explainer" *The Guardian* (online edition, London, 2 December 2013).

David Fisher "GCSB spies Monitored Diplomats in Line for World Trade Organisation job" *The New Zealand Herald* (online edition, Auckland, 23 March 2015).

David Fisher "Police Exploiting Privacy Act" *The New Zealand Herald* (Auckland, 25 March 2015).

Anne Gearan "Report that NSA Collected French Phone Records Causing Diplomatic Headache for US" *The Washington Post* (online ed, Washington DC, 23 October 2013).

Mirren Gidda "Edward Snowden and the NSA files – Timeline" *The Guardian* (online edition, London, 22 June 2013).

Eileen Goodwin "TPP 'Cold War Taking Place By Proxy'" *Otago Daily Times* (online edition, Dunedin, 29 June 2015).

Glenn Greenwald "NSA Collecting Phone Records of Millions of Verizon Customers Daily" *The Guardian* (online edition, London, 6 June 2013).

Chris Griffith "Australians Flock to VPNs to Avoid Data Retention" *The Australian Business Review* (online edition, Sydney, 13 August 2014).

Margot E Kaminski "Don't Keep the Trans-Pacific Partnership Talks Secret" *The New York Times* (online ed, New York, 14 April 2015).

Ian MacLeod "Spy Versus Spy: Australian Security Oversight Holds Lessons for Canada" *The Ottawa Citizen* (online edition, Ottawa, 18 March 2015).

Rebecca Quilliam "Kim Dotcom Loses Search Warrant Fight" *The New Zealand Herald* (online edition, Auckland, 23 December 2014).

James Risen and Mark Landler "Accused of Drug Ties, Afghan Official Worries U.S." *The New York Times* (New York, 27 August 2009).

Frances Robinson "EU Plans Push on Airline Passenger Name Records After Paris Attacks" *Wall Street Journal* (online edition, New York, 9 January 2015).

Matthew RosenBerg and Azam Ahmed "U.S. Aid to Afghans Flows On Despite Warnings of Misuse" *The New York Times* (New York, 30 January 2014).

John Roughan "Spying on WTO Justified by Economic Ambitions" *The New Zealand Herald* (online edition, Auckland, 28 March 2015).

Aman Sharma "Intelligence Agencies Demand 'Blanket Exemption' from Right to Privacy Bill" *The Economic Times* (online edition, Delhi, 2015).

Sabrina Siddiqui "'From Heroes to Villains': Tech Industry faces Bipartisan Backlash in Washington" The Guardian (online edition, Washington, 26 September 2017)

Sabrina Siddiqui and Ben Jacobs "Donald Trump 'Shared Highly Classified Information with Russian Officials'" *The Guardian* (online edition, Washington, 16 May 2017).

Andrew Sparrow "Intelligence Committee Publishes its Report on Privacy and Security: Politics Live Blog" *The Guardian* (online edition, London, 12 March 2015).

Dennis Tegg "Loophole that Legalises Official Snooping" *The New Zealand Herald* (online edition, Auckland, 15 August 2014).

Robert Verkaik "Minister's Admission Links MI5 and MI6 to 'Torture Victim'" *The Independent* (online edition, London, 10 April 2009).

## *Internet Material*

Article 19 "The Johannesburg Principles on National Security, Freedom of Expression and Access to Information" (1996) Article 19 <www.article19.org>.

Julian Assange "What is WikiLeaks" (2006) Wikilieaks <wikileaks.org>.

Aphichat Aumyoo "ASEAN Single Window Initiative" (18 July 2013) New Zealand Ministry of Foreign Affairs and Trade <www.mfat.govt.nz>.

Association of South East Asian Nations “What is the ASEAN Single Window?” (24 October 2017) ASEAN <asw.asean.org>.

Australian Customs and Border Protection Service "Enhanced Trade Solutions 2015" (12 November 2017) Australian Customs and Border Protection Service <www.border.gov.au>.

Australian Cyber Emergency Response Team "Publications" (2015) Australian Cyber Emergency Response Team <www.auscert.org.au>.

Australian Government "Australian National Security" (2015) Australian Government <www.nationalsecurity.gov.au>.

Mike Blanchfield "75 per cent of Canadians unaware of TPP negotiations: poll" (17 June 2015) CTV News <www.ctvnews.ca>.

Eric Bradner "How Secretive is the Trans-Pacific Partnership?" (12 June 2015) CNN Politics <Edition.cnn.com>.

Brunei FM "Indonesia: President Commissions Single Window Export-Import Service" (30 January 2010) Brunei FM <news.brunei.fm>.

Paul Buchanan "Analyst Says NZ Needs More Oversight of Intelligence Agencies" (22 May 2013) Radio New Zealand <www.radionz.co.nz>.

Canadian Associates to Develop Democratic Burma "Parliamentarians Call on ASEAN to Address Rohingya Crisis" (22 April 2015) Euro-Burma Office <www.euro-burma.eu>.

Central Intelligence Agency "South Asia: Afghanistan" Central Intelligence Agency (United States) (24 June 2014) Central Intelligence Agency <www.cia.gov>.

Liat Clark "Five Eyes Intelligence Pact to be Scrutinised by European Court" (9 September 2014) Wired <www.wired.co.uk>.

Jo Coburn "Passenger Name Record: Sharing Airline Passenger Details" (13 February 2015) BBC News <www.bbc.co.uk>.

CITES "Official Documents" (2015) CITES <cites.org>.

Gordon Corera "No Collusion in Torture, says MI6 Chief" (10 August 2009) BBC News <news.bbc.co.uk>.

Gareth Corfield "30,000 London Gun Owners Hit by Met Police 'Data Breach'" (2017) The Register <www.theregister.co.uk>.

Cosette Creamer and Beth A Simmons "Does Self-Reporting Matter? Evidence from the Convention Against Torture" (20 April 2015)Harvard University <scholar.hardvard.edu>.

David Cunliffe "Ahmed Zaoui Statement" (14 September 2007) New Zealand Government <beehive.govt.nz>.

Department of the Prime Minister and Cabinet "National Security System" (2011) Department of the Prime Minister and Cabinet <www.dpmc.govt.nz>.

Department of the Prime Minister and Cabinet "New Zealand's National Security System" (May 2011) Department of the Prime Minister and Cabinet <www.dpmc.govt.nz>.

Department of the Prime Minister and Cabinet "Security in the Government Sector" (2002) Government Communications Security Bureau <www.gcsb.govt.nz>.

DHL Global Forwarding "DHL Global Forwarding Ocean Freight: Beyond Port to Port" (2015) Deutsche Post DHL Group <www.dhl.co.nz>.

Dictionary.com "Big Data" (2017) Dictionary.com <www.dictionary.com>.

Joshua Eaton "Timeline of Edward Snowden's Revelations" (5 June 2013) Al Jazeera <america.aljazeera.com>.

Editorial "John Key hits back at Nicky Hager over GCSB claims" (23 March 2015) Newshub <www.newshub.co.nz>.

Brent Edwards "Spy Watchdog to Investigate GCSB" (31 March 2015) Radio New Zealand <www.radionz.co.nz>.

Embassy of the Republic of Indonesia "RI to Take Advantage of ASEAN Single Window System" (19 September 2010) Embassy of the Republic of Indonesia <embassyofindonesia.org>.

Embassy of the Republic of Indonesia "Trade and Investment News" Embassy of the Republic of Indonesia (30 December 2008) <embassyofindonesia.org>.

Richard Engel "Drugs, Weapons and Mexico" (21 October 2010) MSNBC <dailynightly.msnbc.msn.com>.

Estonian Tax and Customs Board "Customs Formalities Applied with International Postal Consignments" (2012) Estonian Tax and Customs Board <www.emta.ee>.

European Commission "Agencies" (10 November 2017) European Commission <ec.europa.eu>.

European Commission "Alerts and data in the SIS" (10 November 2017) European Commission <ec.europa.eu>.

European Commission "Schengen Information System" (2015) European Commission <ec.europa.eu>.

European Commission "SIRENE cooperation" (10 November 2017) European Commission <ec.europa.eu>.

Lee Ferran "Court: CIA Tortured German During Botched Rendition" ABC News (2012) <abcnews.go.com>.

Rebecca Foley and Bruce Northway "Managing Risk in Customs: Lessons from the New Zealand Customs Service" (2010) World Bank <openknowledge.worldbank.org>.

Foreign & Commonwealth Office "Overseas Security and Justice Assistance Guidance (OSJA): Human Rights" (2017) Foreign & Commonwealth Office <www.gov.uk>.

Foreign Policy Group "The Failed State Index 2011" (17 June 2011) Foreign Policy Group <www.foreignpolicy.com>.

Conor Friedersdorf "Is 'The Five Eyes Alliance' Conspiring to Spy on You?" (25 June 2013) The Atlantic Monthly Group <www.theatlantic.com>.

Sarah L Garcia "Multilateral Cooperation: a New Look at Information Sharing" (2005) The Inter-American Defense Board <library.jid.org>.

Anne Gearan "Spying on France Causes Diplomatic Headache" (22 October 2013) Fairfax Media <www.stuff.co.nz>.

Global Liberty Internet Campaign (GLIC) "Privacy and Human Rights: An International Survey of Privacy Laws and Practice" (2010) GLIC <glic.org>.

Andy Greenberg "Privacy Critics go 0-2 with Congress' Cybersecurity Bills" (26 March 2015) Wired <www.wired.com>.

Graham Greenleaf "Global Tables of Data Privacy Laws and Bills (4rd Ed, January 2015)" (2015) Australasian Legal Information Institute <www2.austlii.edu.au>.

Her Majesty's Revenue and Customs Service "Notice 143: A Guide for International Post Users" (1 February 2014) Her Majesty's Revenue and Customs Service <www.gov.uk>.

Her Majesty's Revenue and Customs Service "About Us" (2008) Her Majesty's Revenue and Customs Service <customs.hmrc.gov.uk>.

Bevan Hurley "DNA database detectives deserve our scrutiny" (14 October 2017) Fairfax Media <www.stuff.co.nz>.

Bevan Hurley, Sam Sherwood and Michael Hayward "Parents upset at police access to blood samples taken from babies" (15 October 2017) Fairfax Media <www.stuff.co.nz>.

Immigration New Zealand "Five Country Conference Questions and Answers" (20 December 2010) Immigration New Zealand <www.immigration.govt.nz>.

Immigration New Zealand "People Travelling to New Zealand: Information for Airlines" (14 August 2014) Immigration New Zealand <www.immigration.govt.nz>.

Immigration New Zealand "Privacy Impact Assessment for Exchange of Information between the New Zealand Department of Labour and the Australian Department of Immigration and Citizenship, as part of the Five Country Conference High Value Data Sharing Protocol" (2010) Immigration New Zealand <www.immigrastion.govt.nz>.

Industrial Control Systems Cyber Emergency Response Team "Standards and References" (2015) Industrial Control Systems Cyber Emergency Response Team <ics-cert.us-cert.gov>.

Insee "Contents of the Sirene Database" (11 November 2017) Insee <www.sirene.fr>.

Inspector-General of Intelligence and Security "Annual Report for the Year Ended 30 June 2017" (2017) Office of the Inspector-General of Intelligence and Security <www.igis.govt.nz>.

International Air Transport Association "Standards, Manuals and Guidelines" (2015) International Air Transport Association <www.iata.org>.

International Telecommunications Union "ICT Regulation Toolkit" (2009) ITU <ictregulationtoolkit.org>.

INTERPOL "Constitution of the ICPO-INTERPOL I/CONS/GA/1956(2008)" (2008) INTERPOL <www.interpol.int>.

INTERPOL "History" (2015) INTERPOL <www.interpol.int>.

INTERPOL "INTERPOL's Rules on the Processing of Data III/IRPD/GA/2011(2016)" (2014) INTERPOL <www.interpol.int>.

INTERPOL "Overview" (2015) INTERPOL <www.interpol.int>.

INTERPOL "Rules on the Control of Information and Access to INTERPOL's Files II.E/RCIA/GA/2004(2009)" (2009) INTERPOL <www.interpol.int>.

Investigatory Powers Tribunal "Investigatory Powers Tribunal Report: 2011-2015" (2016) Investigatory Powers Tribunal <ipt-uk.com>.

Italian State Forest Corps "Operation Marco Polo: An Italian Investigation on the Illegal Trade in Asian Traditional Medicine" (10 February 2004) CITES Secretariat <cites.org>.

Paul Kallender "Japan Tightens Personal Data Protection" (28 March 2005) InfoWorld <infoworld.com>.

Jane Kelsey "Is the GCSB ‘Trade Team’ Spying on NZ's TPPA 'Partners'?" (24 March 2015) Scoop Media <www.scoop.co.nz>.

Bob Kinzel "Despite Welch's Vote, Trans-Pacific Trade Approved By Slim Margin In US House" (12 June 2015) Vermont Public Radio <digital.vpr.net>.

Lloyds Bank "Privacy: How Your Personal Information as Used by Lloyds Banking Group Companies" (2015) Lloyds Bank <www.lloydsbank.com>.

Craig McCulloch "Exporters Welcome Revamped TPP, Critics have Doubts" (13 November 2017) Radio New Zealand <www.rnz.co.nz>.

Ministry of Economy, Trade and Industry "Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information" (12 November 2017) Ministry of Economy, Trade and Industry <www.meti.go.jp>.

Ministry of Foreign Affairs and Trade "Agreement Between the European Union and New Zealand on Cooperation and Mutual Administrative Assistance in Customs Matters" (2017) Ministry of Foreign Affairs and Trade < www.treaties.mfat.govt.nz>.

Ministry of Foreign Affairs and Trade "Text of the Trans-Pacific Partnership" (2015) Ministry of Foreign Affairs and Trade <www.mfat.govt.nz>.

Ministry of Foreign Affairs and Trade "Trans-Pacific Partnership" (2017) Ministry of Foreign Affairs and Trade <www.mfat.govt.nz>.

Montserrat Customs and Excise Department "A Guide to Clearing Air Cargo Through Customs " (2008) Montserrat Customs and Excise Department <customs.gov.ms>.

Musees de grasse "You Are A Private Individual" (2017) Musees de grasse <www.museesdegrasse.com>.

National Archive "Tabular Comparison of 1946 and 1948 Appendices to the US-British Communication Intelligence Agreement (HW80/8)" (1948) United Kingdom National Archives <www.nationalarchives.co.uk>.

National Archives "British-US Communication Intelligence Agreement (HW80/4)" (5 March 1946) United Kingdom National Archives <www.nationalarchives.gov.uk>.

National Archives "Newly Released GCHQ Files: UKUSA Agreement" (1 June 2010) The National Archives <www.nationalarchives.gov.uk>.

National Archives "Outline of Draft British-US Communication Intelligence Agreement (HW80/2)" (1 November 1945) United Kingdom National Archives <www.nationalarchives.gov.uk>.

National Cyber Security Centre "About the National Cyber Security Centre" (2015) National Cyber Security Centre <www.ncsc.govt.nz>.

National Security Agency "Revision of the UKUSA Agreement" (2 September 1954) National Security Agency <www.nsa.gov>.

National Security Agency "Terms of Reference for Negotiating a New COMINT Agreement, 2 September 1954: Memorandum for the Members of USCIB" (21 December 1954) National Security Agency <www.nsa.gov>.

National Security Agency "UKUSA Agreement Release 1940-1956 " (24 June 2010) National Security Agency <www.nsa.gov>.

National Security Council "National Security Council Intelligence Directive No. 11: Security of Information on Intelligence Sources and Methods" (1950) Central Intelligence Agency <foia.cia.gov>.

New Zealand Customs Service "Import Entry Process" (9 July 2015) New Zealand Customs Service <www.customs.govt.nz>.

New Zealand Customs Service "Intelligence-led" (2017) New Zealand Customs Service <www.customs.govt.nz>.

New Zealand Customs Service "Secure Export Scheme" (2015) New Zealand Customs Service <www.nzcs.govt.nz>.

New Zealand Customs Service "Statement of Intent 2012-2015" (2015) New Zealand Customs Service <www.customs.govt.nz>.

New Zealand Customs Service "Statement of Intent 2014-2017" (2014) New Zealand Customs Service <www.customs.govt.nz>.

New Zealand Customs Service "Statement of Intent 2017-2021" (2017) New Zealand Customs Service <www.customs.govt.nz>.

New Zealand Law Commission "Briefing Paper for the Minister Responsible for the New Zealand Law Commission" (2011) New Zealand Law Commission <www.lawcom.govt.nz>.

New Zealand Law Commission "Government Response to Law Commission Report on the Review of the Privacy Act 1993" (2011) New Zealand Law Commission <www.lawcom.govt.nz>.

New Zealand Law Commission "Invasion of Privacy - Penalties and Remedies: Review of the Law of Privacy Stage 3 (NZLC R113)" (2010) New Zealand Law Commission <www.lawcom.govt.nz>.

New Zealand Law Commission "Ministerial Briefing: Information Sharing" (2011) New Zealand Law Commission <www.lawcom.govt.nz>.

New Zealand Law Commission "Public Registers: Review of the Law of Privacy Stage 2 (NZLC R101)" (2008) New Zealand Law Commission <www.lawcom.govt.nz>.

New Zealand Law Commission "Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4 (NZLC IP17)" (2010) New Zealand Law Commission <www.lawcom.govt.nz>.

New Zealand Law Commission "Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4 (R123)" (2011) New Zealand Law Commission <www.lawcom.govt.nz>.

New Zealand Law Commission "The Crown in Court: A review of the Crown Proceedings Act and National Security Information in Proceedings (R135)" (2015) New Zealand Law Commission <www.lawcom.govt.nz>.

New Zealand Law Society "LawTalk Issue 866: More Detail Needed to Support Access to Customs Information" (5 June 2015) New Zealand Law Society <www.lawsociety.co.nz>.

Melanie Newman "Pressure on GCHQ to Disclose Internal Policies After Historic Tribunal Ruling" (6 February 2015) The Bureau of Investigative Journalism <www.thebureauinvestigates.com>.

Office of the Australian Information Commissioner (OAIC) "Privacy Fact Sheet 2: National Privacy Principles" (July 2011) OAIC <www.oaic.gov.au>.

OECD "Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data" (1980) OECD <www.oecd.org>.

OECD "Members and Partners" (2015) OECD <www.oecd.org>.

OECD "Privacy Framework" (2013) OECD <www.oecd.org>.

OECD "Quantitative Assessment of the Benefits of Trade Facilitation TD/TC/WP (2003) 31/FINAL" (13 November 2003) OECD <www.oecd.org>.

Pacific Disaster Centre "Regional Risk Assessment for ASEAN Member States" (21 April 2015) Pacific Disaster Centre <www.pdc.org>.

James Panichi "Debate on PNR Deal Gets Off to Rocky Start in Parliament" (27 February 2015) European Voice <www.europeanvoice.com>.

Jules Polonetsky, Omer Tene and Christopher Wolf "How to Solve the President's Big Data Challenge" (2014) The International Association of Privacy Professionals <www.iapp.org>.

Prime Minister and the Secretary of State for the Home Department "Countering International Terrorism: the United Kingdom's Strategy" (July 2006) United Kingdom Home Office <www.gov.uk>.

Privacy and Civil Liberties Oversight Board "Recommendations Assessment Report" (2015) Privacy and Civil Liberties Oversight Board <www.pclob.gov>.

Privacy and Civil Liberties Oversight Board "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (2014) Privacy and Civil Liberties Oversight Board <www.pclob.gov>.

Privacy and Civil Liberties Oversight Board "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court" (2014) Privacy and Civil Liberties Oversight Board <www.pclob.gov>.

Privacy Commissioner "Guthrie Tests: A Report by the Privacy Commissioner following his Inquiry into the Collection, Retention, Use and Release of Newborn Metabolic Screening Test Samples, Pursuant to Section 13(1)(m) of the Privacy Act 1993" (September 2003) Office of the Privacy Commissioner <www.privacy.org.nz>.

Bart W Schermer "Legal Issues of Single Window Facilities for International Trade" (2007) UNCITRAL <uncitral.org>.

Jon Schwarz "You can't read the TPP and you can't find out who in Congress has" (14 June 2014) The Intercept <firstlook.org>.

Frank Sisto "Privacy Impact Assessment for the Law Enforcement Information Database" (2008) US Department of Homeland Security <dhs.gov>.

Bruce Slane "Centralised Databases: People, Privacy and Planning - a Paper Presented by the Privacy Commissioner to the New Zealand - Australia Health IT Directors meeting" (18 February 1998) Privacy Commissioner <privacy.org.nz>.

Bruce Slane "SIS to Report Publicly for the First Time NZSIS (No 2) Bill" (20 July 1999) Privacy Commissioner <privacy.org.nz>.

Russell G Smith "Trends and Issues in Criminal Justice" (2004) Computer Crime Research Centre<crime-research.org>.

State Services Commission "Personal Information Protection and Public Confidence" (22 December 1998) State Services Commission <ssc.govt.nz>.

TD Bank "Important Information About Your Privacy and Protecting Your Identity" (2015) TD Bank <www.tdbank.com>.

Television New Zealand "Timeline in the Ahmed Zaoui Case" (9 July 2007) Television New Zealand <tvnz.co.nz>.

Trend Micro Incorporated "Cybercriminals Reinvent Methods of Malicious Attacks" (7 July 2008) Help Net Security <www.net-security.org>.

JKT Tsen "Ten years of Single Window Implementation: Lessons Learned for the Future" (13 December 2011) UNECE <unece.org>.

United Kingdom Cabinet Office "Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees" (2010) United Kingdom Cabinet Office <www.gov.uk>.

United Kingdom Cabinet Office “Government Security Classifications 2014” (2014) United Kingdom Cabinet Office <www.gov.uk>.

United Kingdom Home Office "Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference" (2010) United Kingdom Home Office <www.gov.uk>.

United Nations "Afghanistan and the United Nations" (15 January 2015) United Nations <www.un.org>.

UNECE "Trade Facilitation Implementation Guide: Customs Automation" (2015) United Nations Economic Commission for Europe <tfig.unece.org>.

UNECE "Trade Facilitation Implementation Guide: Customs Risk Management and Selectivity" (2015) United Nations Economic Commission for Europe <tfig.unece.org>.

United Nations Office on Drugs and Crime "UN Instruments and Other Relevant International Standards on Money-Laundering and Terrorist Financing" (2015) United Nations Office on Drugs and Crime <www.unodc.org>.

United States Computer Emergency Readiness Team "Publications" (2015)United States Computer Emergency Readiness Team <www.us-cert.gov>.

United States Customs and Border Protection Service "2012 – 2016 Border Patrol Strategic Plan" (2012) United States Customs and Border Protection <www.cbp.gov>.

United States Customs and Border Protection Service "C-TPAT: Customs-Trade Partnership Against Terrorism" (2015) United States Customs and Border Protection Service<www.cpb.gov>.

United States Department of Homeland Security "A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States" (2015) United States Department of Homeland Security <www.dhs.gov>.

United States Department of the Treasury "Foreign Account Tax Compliance Act (FATCA)" (15 May 2017) United States Department of the Treasury <www.treasury.gov>.

(2015) US Bank "Privacy" US Bank<www.usbank.com>.

Andrea Vance "GCSB acted illegally on Kim Dotcom" (2013) Fairfax Media <www.stuff.co.nz>.

Westpac Bank "Privacy Policy" (2015) Westpac Bank <westpac.com.au>.

Phil Williams "Organized Crime and Cybercrime: Synergies, Trends, and Responses" (2001) Computer Crime Research Centre <crime-research.org>.

WCO "Activities and Programmes: National Single Window" (15 May 2017) World Customs Organisation <www.wcoomd.org>.

WCO “Guidelines on Advance Passenger Information (API)” (October 2014) World Customs Organisation <www.wcoomd.org>.

WCO "Model Bilateral Agreement on Mutual Administrative Assistance in Customs Matters" (June 2004) World Customs Organisation <www.wcoomd.org>.

WCO "SAFE Framework of Standards to Secure and Facilitate Global Trade" (June 2012) World Customs Organisation <www.wcoomd.org>.

WCO "The Authorised Economic Operator and the Small and Medium Enterprise" (May 2010) World Customs Organisation <www.wcoomd.org>.

WCO "WCO Cross-Border Regulatory Agencies Customs Data Model: General Information" (2008) World Customs Organisation <www.wcoomd.org>.

WCO "WCO Customs Risk Management Compendium" (2015) World Customs Organisation <www.wcoomd.org>.

WCO "WCO Data Model" (2008) World Customs Organisation <www.wcoomd.org>.

WCO "WCO Data Model Single Window Data Harmonisation" (1 October 2014) World Customs Organisation <www.wcoomd.org>.

WCO "WCO Encourages One-Stop Service at Borders" (9 August 2005) World Customs Organisation <www.wcoomd.org>.

WCO "WCO Profile" (2010) World Customs Organisation <www.wcoomd.org>.

WCO "WCO Research paper No. 17: A Survey of Single Window Implementation" (2011) World Customs Organisation <www.wcoomd.org>.

David Widdowson “Managing Risk in the Customs Context” in Luc De Wulf and Jose B Sokol Customs Modernization Handbook (World Bank, Washington DC, 2005) 91.

WTO "Bali Ministerial Declaration and Decisions" (27 November 2014) WTO <www.wto.org>.

WTO "Preparatory Committee on Trade Facilitation, Agreement on Trade Facilitation WT/L/931" (15 July 2014) United Nations Economic Commission for Europe <tfig.unece.org>.