

<http://researchcommons.waikato.ac.nz/>

Research Commons at the University of Waikato

Copyright Statement:

The digital copy of this thesis is protected by the Copyright Act 1994 (New Zealand).

The thesis may be consulted by you, provided you comply with the provisions of the Act and the following conditions of use:

- Any use you make of these documents or images must be for research or private study purposes only, and you may not make them available to any other person.
- Authors control the copyright of their thesis. You will recognise the author's right to be identified as the author of the thesis, and due acknowledgement will be made to the author where appropriate.
- You will obtain the author's permission before publishing any material from the thesis.

The Waikato Data Privacy Matrix

A Thesis

submitted in partial fulfilment
of the requirements for the Degree
of

Master of Cyber Security

at the

University of Waikato

by

Craig Scoon



THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

©January 2017

Abstract

Data privacy is an expected right of most citizens around the world, but there are many legislative challenges within boundary-less cloud computing and World Wide Web environments. Despite its importance, there is limited research around data privacy law gaps and alignment; the legal side of the security ecosystem seems to be in a constant effort to catch-up. There are recent issues showing a lack of alignment that caused some confusion. An example of this is the ‘right to be forgotten’ case in 2014 that involved a Spanish man and Google Spain. He requested the removal of a link to an article about an auction of his foreclosed home, for a debt that he had subsequently paid. However, misalignment of data privacy laws caused further complications to the case.

This thesis introduces the Waikato Data Privacy Matrix, our global project for alignment of data privacy laws, by focusing on Asia Pacific data privacy laws and its relationships with the European Union and the United States. While much alignment work is already done for the European Union and United States, there is a lack of research on Asia Pacific alignment within its region and across other regions. The Waikato Data Privacy Matrix also suggests potential solutions to address some of the issues that may occur when a breach of data privacy occurs, in order to ensure an individual has their data privacy protected across the boundaries

within the Web. With the increase in data processing and storage across different jurisdictions and regions (e.g. cloud computing services with servers in several countries), the Waikato Data Privacy Matrix empowers businesses using or providing cloud services to understand the different data privacy requirements across the globe - paving the way for increased cloud adoption and usage.

Acknowledgements

I would first like to thank my supervisor Dr Ryan Ko for all the time and support you have given me throughout my University life. My university experience has been hard and sometimes frustrating and I feel there is no way I could have done this without your support and extensive knowledge. In saying that the times weren't all bad and I even had the pleasure of sharing a camel ride with Ryan.

I would also like to thank Associate Professor Wayne Rumbles. Without your guidance and support in the Law side of my degree I would not have been successful. Wayne and Ryan are both amazing teachers and mentors and I feel very fortunate to have had the pleasure of having you both there for me.

Thank you to all members of the Cyber Security Researchers of Waikato (CROW) lab, in particular, Mark Will, Jeff Garae, Sam Shute and Alan Tan. You were a constant source of support throughout this process and helped when I needed people to bounce ideas off when I was stuck, and who put up with my nonsense. Brian Cole was also a great help with engaging with industry.

Also to Cloud Security Alliance for granting me with the scholarship which made this year possible.

Finally, I must express my profound gratitude to my family for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. I owe a lot to my parents for the way they have raised me to always strive for my best and take pride in everything I do. I need to make a special thanks to my wonderful mother Margaret. The best mother in the world who has fully supported me through all of the hard times, not only through completing my Masters degree but my whole life. You have been there to read and check my assignments, which is no easy feat with some of the assignment topics. I am truly grateful for everything you have given me.

This accomplishment would not have been possible without all of you.

Thank you.

I also wish to thank the following experts who have contributed their time and input:

Name	Title - Organisation
Alan Shipman	Director, Group5 Training Limited
Albert Pichlmaier	Senior Manager (DNC/TECH) - Personal Data Protection Authority Singapore
Andrew Scothern	Software Development Manager - R&D - Gallagher
Annelies Moens	Deputy Managing Director - Information Integrity Solutions
Becci Whitton	Team Manager, Policy and Technology - Office of the Privacy Commission
Catherine Blackadar Nelson	Disaster Technologist - Google
Costel Ion	Digital Crime Officer, Research & Innovation - INTERPOL
Elijah Kipsoi	Digital Crime Officer, Research & Innovation - INTERPOL
Erick Borsboom	Security Lead - Ribose
Eric Hibbard	CTO Security & Privacy - Hitachi
Heather Ward	Principal Policy Advisor - National Cyber Policy Office
Joanne Knight	NZ subject matter expert for ISO SC27 WG5 - Identity and Privacy Standards
John Edwards	NZ Privacy Commissioner - Office of the Privacy Commission
Katrine Evans	Senior Associate - Hayman Lawyers
Dr. Ken Barker	Professor - University of Calgary
Dr. Madan Oberoi	Director - Cybercrime Directive - INTERPOL
Dr. Michael Dizon	Lecturer - University of Waikato - Faculty of Law
Michele Drgon	President - Dataprobity
Natsuhiko Sakimura	Senior Researcher - Nomura Research Institute
Neil Sanson	Data Matching Compliance Adviser - Office of the Privacy Commission
Ng Kang Siong	Principal Researcher - MIMOS
Paul Ash	Director - National Cyber Policy Office
Pauline Reich	Professor - Waseda University School of Law
Silvino Schlickmann Junior	Assistant Director, Research & Innovation - INTERPOL
Srinivas Poosarla	Vice President - Infosys
Susan Bennett	Principal - Sibenco
Toshinobu Yasuhira	Digital Crime Officer - INTERPOL
Tuukka Haarni	Lead Auditor - Inspecta

Contents

Acronyms	xiv
1 Introduction	1
1.1 Data Privacy: Boundary-Based Legislation Vs. Boundary-Less Implementation	1
1.2 Example Use Case	3
1.3 Objectives	3
1.4 Scope	4
1.5 Process	6
1.6 Thesis Structure	7
2 Literature Review	8
2.1 Background	8
2.2 Justification	8
2.3 Trans-national Agreements	11
2.4 Safe Harbor to Privacy Shield	12
2.5 Acts, Directives and Regulations	14
2.5.1 Bills and Acts	14
2.5.2 EU Directives and Regulations	14
2.5.2.1 General Data Protection Regulation	15
2.6 Legal Cases	17
2.6.1 Schrems v Data Protection Commissioner	18
2.6.2 Google Spain v Agencia Española de Protección de Datos and Mario Costeja González	19

2.6.3	Apple v FBI	21
2.6.4	The Right to be Forgotten Concept	23
2.7	Related Work in Legal Alignment	24
2.7.1	DLA Piper	24
2.7.2	Forrester Global Heat Map	25
2.7.3	International Data Protection Legislation Matrix	25
2.7.4	Baker & McKenzie's Global Privacy Handbook	26
2.8	Summary	26
3	Methodology	29
3.1	Creation of the Waikato Data Privacy Matrix	29
3.1.1	Control Specification Flowchart	32
3.1.2	Legislation Search Flowchart	34
3.1.3	User Flowchart	34
3.2	Domains	36
3.2.1	Legislative Framework	37
3.2.2	Privacy Body	37
3.2.3	Pre-Collection Process	37
3.2.4	Data Processing	38
3.2.5	Data Storage	38
3.2.6	Spam	38
3.2.7	Interception of Data	39
3.3	Domain Specifications	39
3.4	Extra Additions	40
3.5	Chosen Countries	41
4	Verification and Validation	44
4.1	Verification	44
4.1.1	Vetting Process	44
4.1.2	Verification by Privacy Experts	45
4.1.3	Verification Process	46
4.2	Validation	47
4.3	Verification Timeline	49

4.3.1	Milestones	51
5	Discussion of Results	54
5.1	Expert Feedback	54
5.2	Trends Observed	57
5.2.1	Security	57
5.2.2	Gaps	58
5.2.3	Upcoming Global Trends	61
5.3	Challenges	61
5.3.1	Jurisdictional Differences	61
5.3.1.1	Interpretations	62
5.3.1.2	Definitions	63
5.3.1.3	Language	64
5.3.1.4	Access to Legislation	64
5.3.1.5	China	66
5.3.1.6	United States	67
5.3.1.7	Size of Acts	68
5.3.1.8	No “Catch All” Legislation	68
5.3.1.9	Verification and Validation	69
6	Conclusions	71
6.1	Future Work	72
6.1.1	Sectoral Additions	73
6.1.2	Case Law	73
6.1.3	State Legislation	74
6.1.4	Data Privacy Foundation Inc.	75
7	List of Publications	77
	References	78
	Appendix A	
	Related Background	88
A.1	Cloud Computing	89

A.2 The NSA Leaks	90
A.3 PRISM	92
A.4 New Zealand Cyber Security Strategy	92
A.5 Privacy Shield	93
Appendix B	
Background Chapter Figures	95
Appendix C	
Methodology Chapter Figures	106
Appendix D	
Verification From Experts	110
D.6 Katrine Evans [1]	111
D.7 Neil Sanson [2]	116
D.8 Michael Dizon [3]	117
D.9 Alan Shipman [4]	119
Appendix E	
Additional Results Chapter Figures	120
Appendix F	
Conclusion Figures	125

List of Figures

2.1	Cyber Security Strategy 2015 Goals	9
3.1	Flowchart of the methodology for how the Control Specifications were added	32
3.2	Flowchart of the methodology for searching for Relevant Legislation for applicable sections	33
3.3	Flowchart Showing how a user would use the Waikato Data Privacy Matrix	35
3.4	This map shows the chosen countries	43
4.1	Timeline and Milestones of Waikato Data Privacy Matrix	52
5.1	Example of gaps	59
B.1	A general outline of the stages a Bill will pass through in the legislative process within commonwealth countries [5].	96
B.2	Flowchart of the Federal legislative process in the United States (US)	97
B.3	Flowchart of how legislation passes through the European Union (EU) [6]	98
B.4	Flowchart of New Zealand's legislative process [7]	99

B.5	Example of DLA Piper’s Data Protection Laws of the World Handbook [8] which shows New Zealand (NZ) compared with the US	100
B.6	Example of information for US from Forrester Global Heat Map . .	101
B.7	Example screen shot of the Forrester Global Heat Map [9]	102
B.8	Example of Argentina from the International Data Protection Legislation Matrix [10] produced by the US Department of Commerce	103
B.9	Example summary from the Baker & McKenzie’s Global Privacy Handbook	104
B.10	Example of the Baker & McKenzie’s Global Privacy Handbook showing the comparison of three countries and two topics [11] . . .	105
C.11	Example First Draft of the Waikato Data Privacy Matrix	107
C.12	Example Second Draft of the Waikato Data Privacy Matrix before links to legislation put in	108
C.13	Example of the Waikato Data Privacy Matrix final version	109
E.14	A screen shot of the Australian Privacy Act 1988 online version [12]	121
E.15	A screen shot of the New Zealand Privacy Act 1993 online version [13]	122
E.16	Example of a Generic Legislative Hierarchy which applies to the EU and APAC regions	123
E.17	Example of the United States Legislative Hierarchy	124
F.18	This photo shows the size of the Waikato Data Privacy Matrix, which covers 42 A3 pages when printed	128

F.19 Example of how case law binds lower courts providing facts of the case are the same or similar	129
------------------------------------------------------------------------------------------------------------------	-----

List of Tables

- 3.1 The table outlines the three draft versions of the Waikato Data Privacy Matrix and highlights key changes made between the versions 29

Acronyms

APAC	Asia Pacific
APEC	Asia-Pacific Economic Cooperation
CCM	Cloud Controls Matrix
CJEU	Court of Justice of the European Union
CSA	Cloud Security Alliance
DPMC	Department of the Prime Minister and Cabinet (New Zealand)
EC2	Elastic Compute Cloud
EU	European Union
ENISA	European Union Agency for Network and Information Security
FAQ	Frequently Asked Questions
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
GDPR	General Data Protection Regulation
GCSB	Government Communications Security Bureau
IAPP	International Association of Privacy Professionals
ICT	Information and Communications Technology
iOS	iPhone Operating System
IoT	Internet of Things

ISO	International Organization for Standardization
ITIF	Information Technology and Innovation Foundation
MSC	Master of Cyber Security
NCPO	National Cyber Policy Office (New Zealand)
NPC	National People's Congress (China)
NSA	National Security Agency (US)
NZ	New Zealand
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner (New Zealand)
PDPC	Personal Data Protection Commission
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
US	United States
USC	United States Code
WDPM	Waikato Data Privacy Matrix

Chapter 1

Introduction

1.1 Data Privacy: Boundary-Based Legislation Vs. Boundary-Less Implementation

Privacy of an individual is a widely discussed issue in the legal arena, but with the introduction of cloud services, privacy concerns have also made their way into the computing realm. [14] Laws made by governments can sometimes be confusing to an everyday citizen. In recent years, legislation has been enacted to protect the privacy of an individual or society, but this has come under fire. [15] This has been fuelled by the large amount of media coverage and publicity about leaks of personal data, and breaches of data privacy, including the case of the 2013 National Security Agency (NSA) leaks [16]. See the Related Background Appendix at A.2 for more information about the NSA leaks and PRISM. A result of this publicity has meant an increased awareness in data privacy limitations and rights, which highlighted a need for clarification around trans-national legislation and an effective way of

aligning them with other countries so an everyday user (e.g. consumer, small businesses) can understand any privacy concerns that may relate to them or their data processed or stored by third parties.

The emergence of the Internet of Things (IoT) [17] and the adoption of cloud services [18], presents important research foci towards ensuring users and vendors can put trust in these technologies and services by knowing the requirements of different countries' legislation. The amount of data and personal information stored or transferred to servers across trans-national jurisdictions, in which devices reside, creates a need for a better understanding of global data privacy legislation that may create repercussions for their business or privacy.

The Waikato Data Privacy Matrix (WDPM) is a novel tool for the cloud computing environment. To our best knowledge, there is no solution for directing users to specific parts of legislation relevant to them. Current tools [9] [8] simply summarise the legal perspectives on data privacy, and explain the comparisons between two or more countries at a time.

One simple example of variations in legislation across countries, is looking at the differences of the “sensitive data” definition. Throughout the Asia Pacific (APAC) countries surveyed in our research (this is discussed further in Section 3.5), China, Australia and Malaysia have a definition for “sensitive data” while New Zealand and Singapore do not define this. A global alignment will uncover these types of gaps for users in different countries.

1.2 Example Use Case

The following use case is a hypothetical example to show an instance where the WDPM would be useful.

A recent start up company, 'Data Storage Solutions Group' (DSSG), has a business which offers cheaper and more reliable data storage than their Australian competitors. They are a local data centre within their residing country of Australia. Within a few months, DSSG have thousands of new clients in Australia using their data centres to store different forms of data. Word has spread to the US about the reliable service DSSG offers. With all the excess traffic from the US, DSSG has decided to open a new data centre in Silicon Valley. DSSG spent a considerable amount of time prior to setting up the company to ensure they met the Australian privacy principles. With uncertainty and a lack of the law in the US, they turn to the WDPM to give them guidance.

By using the WDPM, they are able to save money and man-hours by quickly comparing and aligning the laws in Australia, with the laws in the US, and avoiding any serious repercussions on their business. Luckily, thanks to the WDPM, DSSG can successfully open their new data centre and maintain their high standard of data privacy protection for storage.

1.3 Objectives

The objective of the WDPM is to create a global alignment of data privacy legislation that will allow users and providers of cloud services to see how other jurisdictions around the world compare. The WDPM needs to provide an easy

way to cross reference different trans-national legislation that will align with a set of predefined domain areas. This will assist a user to see what laws are governing their data wherever in the world that data may be located. The WDPM will also be able to be utilised by governments, and in particular the legislature, to see gaps which may appear in their own legislation and allow them to propose changes to improve or align with the rest of the countries.

The WDPM will also need to be easily accessible to any user, at any time, so any user or vendor of cloud services can be directed to a specific legislation which will help them to answer any questions or worries they might be facing. The WDPM will also help clarify if a certain aspect of data privacy means the same thing across the regions around the world.

The final product will be a Rosetta Stone-like matrix [19] which will represent major cloud-hosting countries in the world. This tool has a wide reaching targeted user base, so it is vital that it is accessible to readers with limited or no legal expertise, and free-to-use for vendors and users of cloud services.

1.4 Scope

The scope of this research is focused on looking at a global alignment of data privacy legislation within the following regions:

- APAC
 - NZ
 - Australia
 - Singapore

- Malaysia
- China
- EU
 - United Kingdom (UK)
 - France
 - Sweden
 - Germany
 - Poland
 - Estonia
- Americas
 - US
 - Canada

The countries included in the WDPM have been chosen as eight out of twelve of them are listed in the top twenty major cloud hosting countries. New Zealand was added as the research is being conducted in New Zealand and aims to aid with the cloud computing growth and technology exports of the country. [20] The research is also being supported by funding from the STRATUS [21] project.

The focus of the research is on data privacy legislation relating to cloud technologies and how data can be processed in a cloud environment. Data privacy plays a major part in cloud services and how new IoT devices are connected to the cloud to store or process data.

The original scope for this research was looking at data privacy as a whole which

covers a variety of types, for example, health specific and finance specific data. After some initial research the scope was refined to cover general data privacy, which meant health specific and finance specific data fell outside the scope of this research, but these will be touched on in Future Work at Section 6.1.1.

The research focuses on national legislation which means that only the top level legislation is looked at, so when researching the US, only their federal legislation is considered. Most countries also have state, sectoral and local legislation but this will not be included in this research due to resource constraints.

1.5 Process

The research process involved in the WDPM is different to a typical Master of Cyber Security (MCS), where the research conducted is validated either by experiments or through user testing. However, because the WDPM is a tool for aligning legislation from different parts of the world, the validation needs to come from experts and legal professionals within each of the targeted countries.

Once the WDPM is completed, the final part will be seeking validation to ensure that the sections which have been referred to, are correct and there is no other legislation that has been missed.

This validation is different to a typical user test, as with those tests the data is collected and analysed by the researcher. With the validation for the WDPM, the research will need to be heavily scrutinised by a group of professionals from all over the world. The hardest part about this research was finding the right people for the validation.

1.6 Thesis Structure

Chapter two will discuss the background information to this research. This will cover relevant literature, background into some events that have shaped the data privacy landscape, legal cases, current related tools and some background on legislation.

Chapter three will discuss our methodology, different domains and domain specifications which make up the WDPM, why the countries from the APAC, the EU and the US were chosen.

Chapter four will discuss the timeline of the verification and validation process the WDPM has taken.

Chapter five will discuss results of the research and challenges that occurred during the research. It also covers challenges around reading and interpreting foreign legislation, locating and accessing legislation.

Chapter six will conclude the research so far and suggest areas for Future Work.

Chapter 2

Literature Review

2.1 Background

This section will discuss the need for the WDPM and other work related to the WDPM.

2.2 Justification

Many users of cloud services do not have a legal background or legal understanding. Cloud services have been incorporated into everyday life, and the geographical boundaries which once contained a legal jurisdiction are now being blurred. The background of cloud computing is further discussed in Related Background Appendix at A.1.

Legislation is an important function in society, set down by the legislature, to govern what are acceptable behaviours, and punishments if these behaviours are not followed.

Cloud users and vendors need to know what legislation will impact on them and their data, wherever it is in the world.

The Department of the Prime Minister and Cabinet (DPMC) in New Zealand released the updated Cyber Security strategy, on December 10 2015, replacing the 2011 version. The strategy outlines the government's response to addressing the threat of cybercrime to New Zealanders. Connect Smart conducted a survey in 2014 on cyber security practises; 83% of those surveyed said they had experienced a data breach in some way (22% saying they had e-mail accounts compromised). The scary side to that statistic is 61% of those did nothing to change their behaviour. [22] The new version has four principles:



Figure 2.1: Cyber Security Strategy 2015 Goals

- Partnerships are essential
- Economic growth is enabled
- National security is upheld
- Human rights are protected online

The strategy outlines four intersecting goals shown in Figure 2.1. Further explanation of these principles is found in Related Background Appendix at A.4.

New Zealand is not the only country to release a new cyber security strategy [23]. Australia released their four-year strategy in April 2016 which outlines five themes:

- A national cyber partnership
- Strong cyber defences
- Global responsibility and influence
- Growth and innovation
- A cyber smart nation

The Australian and New Zealand strategies have similar goals in mind - ultimately educating citizens, and providing tools and international co-operation.

Thousands of new businesses are started every year, some of these will not even get off the ground and out of the ones that do, around 10% will fail within the first year and around 70% will fail within five years. [24] One of the biggest points of failure comes down to the business revenue. Even a company which is semi established that needs to break out into an overseas market to get more customers, may not have enough revenue to hire a legal team or even a single professional,

to give them all of the legal advice to successfully launch their business in an overseas jurisdiction. Legal bills can be very expensive. Although legislation is freely available in most countries around the world it may not be easy to navigate.

The WDPM addresses the needs, outlined in this section, by providing a free easy-to-follow tool for identifying which data privacy laws may affect a user's data in another jurisdiction. For a small business owner or even an established business it can be a costly exercise to get legal advice. The WDPM can minimise some costs by pointing the user in the right direction, saving on labour costs.

2.3 Trans-national Agreements

To protect data privacy within the EU, the Data Protection Directive¹ [25] was enacted in 1995. This directive only applied to a participating EU member country which meant that data could not be transferred outside of the EU. The EU-US Umbrella Agreement is a framework to enable co-operation between law enforcement efforts between the EU and US which covers all categories of personal data exchanged between the two countries. This agreement is purely for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism [26]. The Safe Harbor Agreement which was launched in 2000, was an important step towards trans-national partnerships. It was set up to allow commercial companies to transfer data from the EU to the US and store the data within

¹Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

the US. The agreement allowed for a country outside of the EU to transfer data as long as they could provide an adequate level of protection, which was of a similar level to the EU regulations. There were some conditions for a company to have this ability. A company in the US would have to be certified to be part of the agreement. They were able to self-certify or outsource the certification to a third party, where the company must comply with the seven principles in the Agreement, as well as a set of 15 Frequently Asked Questions. The Safe Harbor principles were an expansion on the original 1980 Organization for Economic Cooperation and Development (OECD) recommendations towards privacy principles for personal data [27]. Providing the company complies with the seven principles and the Frequently Asked Questions, along with the EU Data Protection Directive, Swiss requirements, and a \$100 yearly fee, the company could be part of the Safe Harbor Agreement. This registration method is not stringent and has the possibility for misuse. However, the Safe Harbor Agreement was ruled invalid, in October 2015, by the Court of Justice of the European Union (CJEU) following in the wake of the Snowden leaks, and after the case of Max Schrems covered in 2.6.1.

2.4 Safe Harbor to Privacy Shield

The Safe Harbor Agreement was launched in 2000 after the European Commission and the Department of Commerce of the United States agreed it had adequate protection for transferring data from the EU to the US. Thirteen years later, the Safe Harbor Agreement began to come under fire in the wake of the Snowden leaks, and by October 2015 the CJEU had declared the Safe Harbor invalid, after the case of Max Schrems which will be covered in 2.6.1.

After the invalidation, a draft of the new EU-US Privacy Shield [28] emerged. The draft Privacy Shield was announced in February 2016, and is an adaption of the Safe Harbor Agreement. In a press release in February 2016 the European Commission stated that the new Privacy Shield would “provide stronger obligations on companies in the EU to protect the personal data of Europeans and stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission, including through increased co-operation with European Data Protection Authorities.” [29] Three new elements were included in the new Privacy Shield framework.

- Strong obligations on companies handling Europeans’ personal data, and robust enforcement
- Clear safeguards and transparency obligations on US government access
- Effective protection of EU citizens’ rights with several redress possibilities

The Privacy Shield was signed off on July 8 2016 by the European Commission and the Department of Commerce of the United States. The new and approved version of the Privacy Shield contains numerous clarifications for the privacy principles. These principles can be found in Related Background Appendix at A.5.

The Privacy Shield was open to companies from August 1 2016, so by August 2017 the questions around how legitimate this Privacy Shield will be, should be answered. All going well, it should be able to restore and start to rebuild trust with the citizens around the use, protection, and stewardship of data. [30]

2.5 Acts, Directives and Regulations

Every country has legislation which is enacted by Parliament; these are usually the highest forms of law within a country. For member countries of the EU they also have EU Guidelines and EU Regulations. This section will explain how each of these documents work in the legal framework.

2.5.1 Bills and Acts

A Bill is a proposed Act which is introduced into parliament. The Bill passes through several stages; an example of the New Zealand legislative process can be seen in Background Figures Appendix at Figure B.4. Once the third reading has been passed, the Bill has been passed. The final step in the Bill is to receive royal assent by the Sovereign - in the case of New Zealand this is done by the Governor General. Assent will give the Bill the final seal of approval and a date when it will come into force in that jurisdiction. The Bill is now an Act. [7]

This process is similar in other countries. An example of the general legislative process for other commonwealth countries is shown in Background Figures Appendix at Figure B.1, and the legislative process for Federal Bills for the US is shown in Background Figures Appendix at Figure B.2. Once the bill receives Royal assent and comes into force, it is a legally binding piece of legislation.

2.5.2 EU Directives and Regulations

The EU creates several types of legal Acts for member countries to abide by or use. The main two are directives and regulations.

When drafting regulations and directives, the EU follows similar processes to other

government legislative processes; the EU legislative process [6] can be seen in Background Figures Appendix at Figure B.3.

An EU directive affects all member countries. The directive will outline a certain goal which the member countries must achieve. It is then up to each country how they implement it into current legislation. Some countries may choose to amend current legislation or create a new piece of legislation to attain what the EU wants to achieve. The country will have a set time in which they need to put it into law; this is outlined in the directive itself. National authorities need to communicate how this is achieved to the European Commission. [31]

An EU regulation is different to the directive. A regulation is immediately binding on all member states once passed by the EU. This means a member country does not have to incorporate it into law. EU regulations are a good way for the EU to set legal standards for all of their member countries.

2.5.2.1 General Data Protection Regulation

Currently in the EU there are numerous directives in place which aim to protect personal data. The EU Data Protection Directive² [25], which is the main document within the EU for data protection regulates how data can be processed within the EU. In addition there are two other directives which compliment the Data Protection Directive. The first of these is the 2009 E-Privacy Directive³ which

²Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

³Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on co-operation between national

replaced the former 2002 E-Privacy directive [32], and the second one is the Data Retention Directive⁴ [33].

The General Data Protection Regulation (GDPR)⁵ is a new regulation from the EU that will come into force from 25 May 2018, replacing the existing EU Data Protection Directive. The GDPR will help to strengthen and unify data protection for individuals who reside within the EU.

The GDPR will introduce or further define the following areas: [34]

- Increased Territorial Scope
- Tougher Sanctions
- Consent
- Breach Notification
- Right to Access
- Right to be Forgotten
- Data Portability
- Privacy by Design

authorities responsible for the enforcement of consumer protection laws

⁴Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

⁵Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

- Data Protection Officers

Once in force, the GDPR will be legally binding on all member states of the EU. This will also extend the scope to *all* organisations who may operate within the EU or process data of EU citizens whether they are headquartered there or not. [35] [36]

There has been much discussion around the effects the GDPR will have on the data privacy landscape. The general consensus is that the GDPR will have a positive effect. The new principles in the GDPR aim to give back the control to citizens over their data. The GDPR will set the new standard for data privacy.

The WDPM will need to be updated once the GDPR comes into force, however the key point here is that that all data privacy legislation currently enforced within the EU will come from the GDPR, meaning a user will only need one document to reference. The WDPM is a tool to allow users to compare data privacy laws across the globe, so even though the GDPR will be the one document within the EU it will still need to align with the rest of the non-EU countries to see how their data privacy legislation aligns.

2.6 Legal Cases

This section will cover some of the legal issues and cases from around the world which have increased the profile of data privacy in recent years.

2.6.1 Schrems v Data Protection Commissioner

The Schrems⁶ case is probably the biggest and most important privacy case in recent history, resulting in the invalidation of the Safe Harbor Agreement.

Maximillian Schrems, an Austrian law student and privacy activist, was studying abroad at Santa Clara University, completing his PHD, where he wrote a term paper on Facebook's lack of awareness of European privacy law. [37] During his research, Mr Schrems sent a request to Facebook for their records on him and received a CD with over 1,200 pages of data. This sparked the start of his journey down the road that would eventually lead him to the CJEU.

Mr Schrems then filed 23 complaints, against Facebook, to the Irish Data Protection Commissioner. These complaints related to the level of protection which was provided for data in the US. Most of Mr Schrems data for Facebook was transferred from one of Facebook's subsidiary companies in Ireland through to servers in the US, where his data was then processed. This was permitted through the Safe Harbor Agreement.

The complaints made by Mr Schrems further added concerns to the lack of protection for data offered in the US previously highlighted by the release of the documents in 2013 by Edward Snowden around the spying of the NSA. [38]

After the previous 22 complaints were ignored by the Irish Data Protection Authority, the 23rd complaint reached CJEU, where the Court ruled the Safe Harbor Agreement invalid [38]. This decision put many of the 4600 US companies [39], who relied on the Safe Harbor Agreement, in a state of limbo and scrambling to find a way

⁶Case C-362/14 Schrems V. Data Protection Commissioner [2015] ICLR

to provide alternative guarantees for customers to continue their services lawfully. [40]

2.6.2 Google Spain v Agencia Española de Protección de Datos and Mario Costeja González

This Google case⁷ was another important privacy case which resulted in the new EU ‘Right to be Forgotten’ ruling. [41]

In 1998 a Spanish citizen, Mario González, had two short articles published about him by a Spanish newspaper - La Vanguardia. The newspaper reported Mr González’s home was to be auctioned to pay off his social security debts. Subsequently, these two articles were published on the Internet. Twelve years later in 2010, Mr González made a complaint to the national data protection agency in Spain against the newspaper, as well as Google Spain and Google Inc. He alleged that when any Internet user typed his name into a Google search engine, they would see the two articles published in 1998. Mr González had since rectified these issues and moved on with his life, making these articles now irrelevant; yet, the articles were still available, which he argued were prejudicial to his present and future living.

Mr González requested all personal information relating to him be either removed from the newspaper or the pages in question amended. [42] He then requested Google Spain and Google Inc. to remove or conceal his personal data, so it would not appear in the search results nor in the links to the newspaper. [40]

⁷Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González [2014] C-131/12

The Spanish Court referred this case to the CJEU where it ruled in favour of Mr González, and he won the right for Google Spain and Google Inc. to remove the links from online circulation; however, the articles are still online but are harder to find now with the links gone.

The judgement relied on three main points. The most significant was reference to Article 12 of the EU Data Protection Directive:

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in

compliance with (b), unless this proves impossible or involves a disproportionate effort.

Mr González set out to have information removed, about him, from search engines. This happened, but at the same time had much bigger ramifications for data privacy. The ‘right to be forgotten’ is discussed further in 2.6.4.

2.6.3 Apple v FBI

To give some background on why this case is important to the data privacy debate - in early December 2015 a husband and wife walked into the building of the Inland Regional Centre in San Bernardino, California, to carry out a terrorist attack. They shot and killed 14 people and seriously injured a further 22 people. The two attackers were then shot by police. [43] The police seized the iPhone 5C of one of the shooters.

Once the FBI had the iPhone, they had ten attempts to guess the password before the data on the phone would be erased. The FBI filed a motion to compel Apple to help them access the contents of the phone by bypassing the security. The Judge ordered Apple to provide “reasonable technical assistance”. For Apple to allow this type of access, they would have to write a completely new version of their iPhone Operating System (iOS). The new version would essentially allow a backdoor into the iPhone by bypassing the security features built in to the current iOS, allowing the FBI to use a brute force attack to crack the pass code to the phone. [44]

Although Apple said it was possible for them to build the backdoor into their system, they said it was too dangerous and once it was created anyone could use it to gain access to an iPhone. Apple has said they regularly receive requests from law enforcement agencies asking for their help to unlock phones, but have not done this, keeping their customers' privacy their priority.

The FBI managed to unlock the phone, through the use of a third-party, a week before the trial was set to be heard. The FBI has never confirmed how they accessed the phone or which third-party helped them. [45]

The publicity which came out of this case was enormous. In recent years, the US Government has attempted to get Apple and other technology companies to build a form of backdoor into their products, so law enforcement agencies have the ability to bypass the security measures where a phone is involved in an investigation. Apple changed their software in 2014 to ensure their phones could not be unlocked or decrypted. [46] This was a reassuring step for Apple customers, showing that their privacy, and privacy of their data, was important to the company.

“ While we believe the FBI’s intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect. ”

Tim Cook, *Chief Executive Officer of Apple*

2.6.4 The Right to be Forgotten Concept

The ‘right to be forgotten’ is a concept where an individual within the EU has the ability to request search engines remove links to pages that detail certain information about a person which may be inadequate, irrelevant or no longer relevant. This issue, relating to a person’s right to privacy, which came out of the Google Spain case, referred to earlier in 2.6.2 [47], not only affect Google search engine but any search engine which holds a “presence” in the EU, including both Yahoo and Bing.[48]

Currently the ‘right to be forgotten’ only applies to individuals (does not cover companies), living within a member country of the European Union which includes all nationalities residing within the EU. The ‘right to be forgotten’ has been limited by the CJEU. An individual may refer to any person, including celebrities or other people who live in the public eye, although they would still come under the right to be forgotten, this may not guarantee they can be forgotten. The CJEU has specified that search engines must consider the public’s right to information as it is of more importance when dealing with someone in the public eye. Although they may want something removed, they may not be able to have that, due to their position in society.

There may be exceptions to this which could include scams that are the kind of public interest items Google has said will be excluded from ‘right to be forgotten’. Professional malpractice, criminal convictions, or public conduct of government officials would also fall under this exception. [49]

The Court has made it clear that journalistic work must not be touched; it is to

be protected. [49]

For someone to be forgotten, a form is filled out and submitted to Google. If successful, the link to the page would be removed but this only applies to search engines within the EU. If Alice lives in Sweden and was to have something removed, Bob would not be able to see it on Google.fr (France) and Google.ge (Germany), but if it was to be looked up on Google.co.nz it would still be visible. [48]

Although the form can help to get the correct information to Google, there are some issues. If someone has two variations of their name, for instance “Matt Smith” and “Matthew Smith”, the form will only allow for one of these to be removed. This means two forms would need to be filled out. [50]

In 2012 European Union Agency for Network and Information Security (ENSISA) published a paper outlining the pros and cons of the new Bill that was being looked at which would later become the ‘right to be forgotten’. It also laid out the technical aspects of how it could be enforced. [51]

2.7 Related Work in Legal Alignment

This section will cover other tools which are currently available on data privacy and how they compare to the WDPM.

2.7.1 DLA Piper

The DLA Piper Data Protection Laws of the World Handbook [8] was launched in 2012. The handbook allows a user to choose two of the 89 countries and compare

data privacy legislation. This website is helpful to a user to give them some idea of relevant legislation in the countries specified; however, it will mostly give the main piece of legislation relating to data privacy. The handbook then summarises the selected topic, for example, if the user clicks on “Authority” it will give an overview of who the authority is. In New Zealand’s case it just gives contact details for the Office of the Privacy Commissioner.

An example of the DLA Piper handbook is shown in Background Figures Appendix at Figure B.5.

2.7.2 Forrester Global Heat Map

The Forrester Global Heat Map [9] gives a user minimal access without registering for the site. Once registered, a user can buy the report for \$499USD. [52] The heat map shown in Background Figures Appendix at Figure B.7 shows a user the levels of protection in the countries, by utilising different colours to represent different levels of protection. Not all of the countries are represented for free and the user does not get any usable information. Of the seven countries that can be clicked on - Russia, Taiwan, China, Singapore, Thailand, United Kingdom and the US - only the United Kingdom and US give information which is not helpful to the user. This can be seen in Background Figures Appendix at Figure B.6.

2.7.3 International Data Protection Legislation Matrix

The International Data Protection Legislation Matrix [10] was developed by the US Department of Commerce and has not been updated since 2005. It is a table of 51 Areas which includes 50 countries and the EU (it does not include the US). It lists

the relevant legislation, and a hyperlink to that legislation. The document then tells the user the status of the legislation and some key details about the legislation. An example of the document is shown in Background Figures Appendix at Figure B.8.

2.7.4 Baker & McKenzie’s Global Privacy Handbook

This handbook [11] is written and updated by Baker & McKenzie, a global law firm with offices in 47 countries. [53] The user can utilise their tool to select and compare a single country or multiple countries, out of the available 56 countries. The user can then select a single topic or multiple topics to view and compare. The application will then give the user a summary of the legislation, this is shown in Background Figures Appendix at Figure B.9. It does not mention which legislation is used or is applicable in the country. An example of the application is shown in Background Figures Appendix at Figure B.10.

2.8 Summary

The literature has shown that recent events have increased public interest and awareness of privacy in the cloud environment, towards processing and access to data. The NSA leaks in 2013 were a major wake up call, to not only the US public but the rest of the world, to take back control of their data, and find ways to ensure rights and freedoms were being protected. A result of this was seen through the Schrems case mentioned at section 2.6.1 which invalidated the 15 year old Safe Harbor Agreement between the EU and US because of a lack of security over data being transferred.

The literature suggests data privacy is a topic which had come up frequently during the previous decade.

There is limited related work in the area of data privacy tools. The research outlined in this chapter has covered some of the available tools for comparing data privacy legislation, and touched on some of the key events that have contributed to the data privacy debate and helped create the WDPM.

The tools mentioned have one thing in common - they all give a summary of the relevant law. Although some users may be after a quick general summary, that is all it is, a summary of how someone or a group has interpreted the legislation. Legislation may not always be clear and a summary may not be correct for all parties. A user may need to read the section for themselves to see if it will apply to them and their situation.

From these tools there is only one (International Data Protection Legislation Matrix) which links a user to the relevant legislation, but this is the tool created by the US Department of Commerce, and it has not been updated since 2005. Although it does link to some of the legislation, either the links may no longer work or the legislation may now be outdated and no longer relevant.

Either these tools do not give the user the titles of the relevant legislation so they can search for them themselves or they only give one or two titles of legislation to look at, which is not entirely helpful when legislation is spread throughout multiple pieces of legislation; this will be covered more in Chapter 5.

It is important that a user is aware of all relevant legislation, relating to privacy of their data, which may have some impact on them or on their choices. The Global Privacy Handbook does the best job of allowing a user to compare multiple

legislation and topics, but lacks directing the user to the relevant legislation and sections.

The literature and related work had a significant impact on the design and implementation of the WDPM which will be discussed further in Chapter 3. The WDPM aims to address the gaps and issues which have been highlighted by some of the recent events outlined in this chapter.

Chapter 3

Methodology

This chapter will look at the methodology behind the creation of the WDPM. It will cover the domains and how the control specifications were created.

3.1 Creation of the Waikato Data Privacy Matrix

Through the research into automating governance mapping, with the Cloud Controls Matrix (CCM) in 2014, Dr. Ko realised that the crux of the alignment problem for companies not only spanned areas related to governance and control, but also the law.

Although standards and controls are important parts of how organisations function, legislation plays a major part in how and what decisions are made. The WDPM was created based on the fact that standards are advised best practises and are not binding on an organisation, whereas legislation is binding and must be followed by everyone under that jurisdiction.

Table 3.1: The table outlines the three draft versions of the Waikato Data Privacy Matrix and highlights key changes made between the versions

Key Changes to WDPM Versions			
Features	Version 1	Version 2	Version 3
Legislation and Section Information	Yes/No with section referenced	Section Referenced and Notes column	Section Referenced and Notes column
Access to Legislation	Title of document in text	Title of document in text	Title of document hyperlinked to document
Flow of topics	39 ‘Element Present’	7 Domains with 54 control specifications	7 Domains with 54 control specifications

The creation of the WDPM evolved over many months and went through a variety of iterations. The first draft of the WDPM can be seen in Methodology Figures Appendix at Figure C.11. The first version tried to give a user a yes or no answer to a question they had, in this version referred to as ‘Element Present’. The next column then directed the user to the relevant legislation. After this version was completed it was noted that it did not give the user enough information and there needed to be a better flow of the ‘Element Present’ column.

Version two of the WDPM rectified these previous issues by adding the domains and an extra column for ‘Notes’. The Notes column allowed for extra notes to

be added for example, if a country didn't have legislation in place but advised on some best practice. The second draft is shown in Methodology Figures Appendix at Figure C.12. When the second version was finished it was given to selected people who did not know much about the WDPM, and feedback received from that was to be able to link to the legislation directly. Version three is shown in Methodology Figures Appendix at Figure C.13 where the addition of links to the main pages of legislation were added for the user to click on.

The domains and domain specifications selected were chosen as best effort; there was no scientific way to choose what each domain would cover or how many there would be.

Although there have only been three main versions of the WDPM many alterations have been made to them, these have included colour coding domains, adding the domain code, formatting, spelling and adding links or sections.

3.1.1 Control Specification Flowchart

The flowchart in Figure 3.1 shows how the control specifications were chosen, to add to the WDPM. As seen in the flowchart, control specifications were added while reading through a piece of legislation for a specific topic, for example, ‘if consent is required from an individual’ and something from another country came up which had not yet been seen, and if it was relevant to data privacy, it would be added to the control specifications.

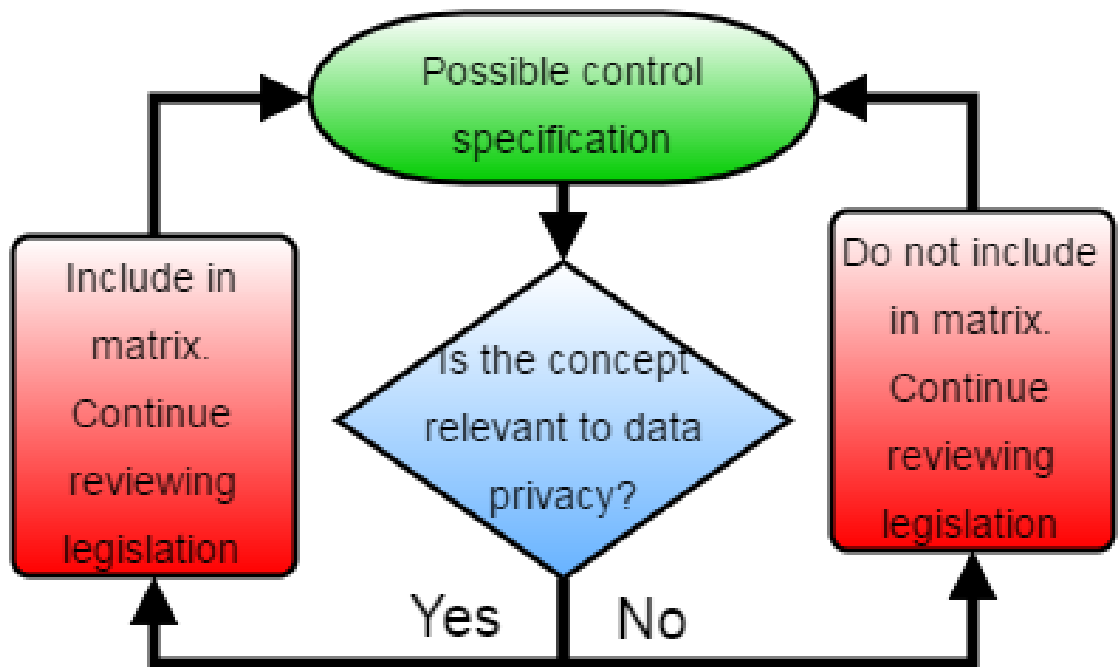


Figure 3.1: Flowchart of the methodology for how the Control Specifications were added

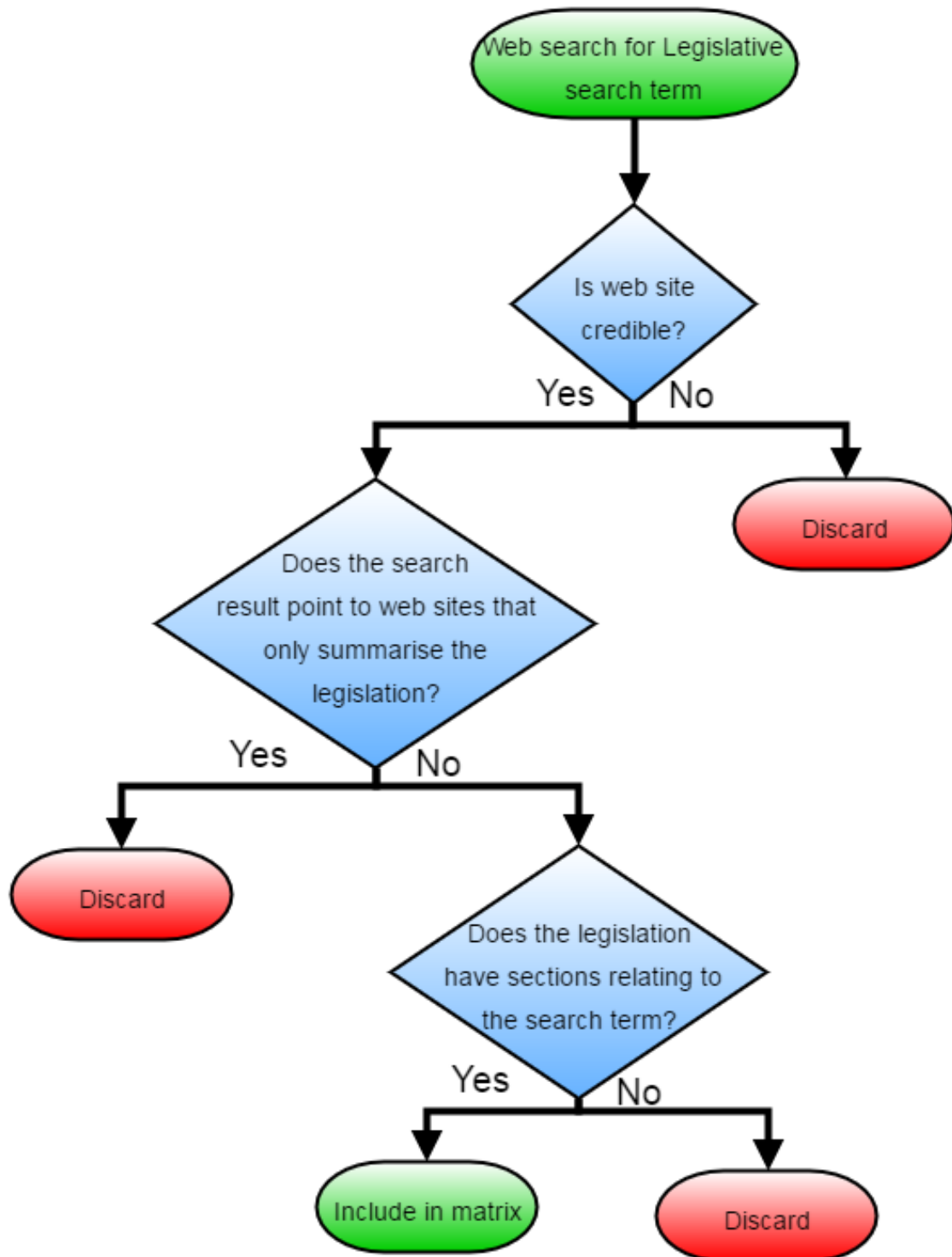


Figure 3.2: Flowchart of the methodology for searching for Relevant Legislation for applicable sections

3.1.2 Legislation Search Flowchart

The flowchart in Figure 3.2 shows how relevant legislation was searched before the section was added to the WDPM. A search term was entered into a search engine, for example, ‘is consent required in NZ to collect data’. The results were then looked at for credibility. The web site was deemed credible and if it had a government domain (e.g. .govt.nz, .gov.au, .gov.uk), if it had been linked to from another government department or if the web site was hosted or written by a recognised law firm or privacy group (e.g. Baker & McKenzie, DLA Piper, International Association of Privacy Professionals (IAPP)). If the web site was not credible it would be discarded. If it was credible and it showed the full legislation then providing it included a section relating to the search term, it was included. If the web site only summarised the legislation it was not included.

3.1.3 User Flowchart

The flowchart in Figure 3.3 shows how a user uses the WDPM. The user starts with some kind of query - “Is my consent required for someone to obtain my data?” The user then looks through the WDPM at the domain controls to find a relevant domain, in this example they would be looking at the pre-collection domain. The user then looks through the domain identified for a domain specification which relates to their query. Once they find the relevant domain specification, the user moves right on the WDPM to find the relevant country for the query to see if there is a section and legislation listed for them to look at. If there is no entry it means the country does not have any legislation in place for that query.

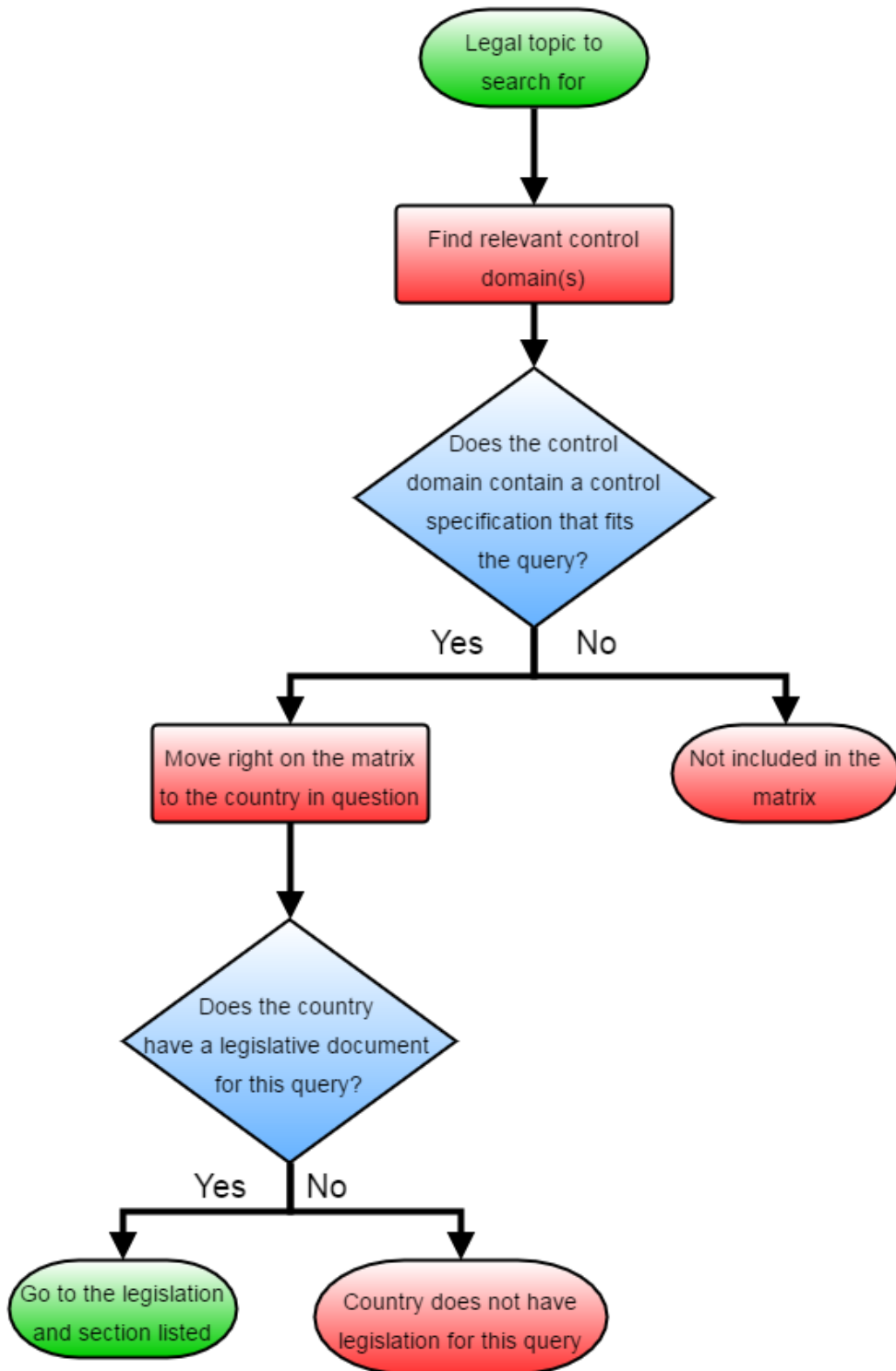


Figure 3.3: Flowchart Showing how a user would use the Waikato Data Privacy Matrix

3.2 Domains

It was essential that the WDPM covered key areas of legal issues relating to privacy. The control domains were created as a way to group similar issues into domains for easy access for the user. This section will outline the domains that have been included in the WDPM, and the purpose they have in the overall picture.

The domains were created after the first draft was completed. This draft only had a list of possible questions/statements people may want to query. After completion of the first draft, it was noted that the WDPM did not really align with one of the key goals of being user friendly, and also seemed to be hard to follow. This led to the second and more revamped version which introduced the control domains. To achieve a more cohesive layout the questions/statements were arranged by common themes into groups; the themes then became the control domains. These domains have been ordered in a logical flow to guide the user from the starting key aspects:

- Legislative Framework
- Privacy Body
- Pre Collection Process
- Data Processing
- Data Storage
- Spam
- Interception of Data

3.2.1 Legislative Framework

The legislative framework domain is the first and most important domain for the matrix to be able to function as it was intended - to give a user legal guidance. The domain sets out the key legislative documents which either directly relate to data privacy or have some sections in them which also contribute to data privacy. This domain is vital to the matrix, as a country needs to have some sort of legislative framework in place so its citizens and visitors know what is allowed or not allowed. As well as understanding rules, people also need to know what kind of punishments are possible if the legislation is not followed.

3.2.2 Privacy Body

The privacy body domain gives the user some guidance on who oversees privacy concerns within the country. It is important that the user knows where they can go, or who they can contact if there has been a breach of privacy. Some of the privacy bodies offer advice or directly handle any complaints made relating to privacy.

3.2.3 Pre-Collection Process

The pre-collection process covers main concerns that a user may have before giving up their data. This is important, for example, when a user signs up to a cloud service like Dropbox, [54] they need to know what they are giving consent to. This domain will help a user see what is required before any data is actually collected from a cloud provider or another party who is permitted to collect data from individuals.

3.2.4 Data Processing

Data processing is a key component of cloud services; it covers how and where data can be processed by the party. These cloud providers cross physical geographical jurisdictional boundaries, and this is the area which raises the most questions.

This domain will guide a user to a better understanding of what legislation is in place to protect their data in this grey area of law.

3.2.5 Data Storage

Similar to the data processing domain, the data storage domain is of similar interest as it looks at areas around how data can be stored by the party processing it. Many questions have arisen about the possibility of data being stored in a country other than where the data was collected or processed. This may be a crucial step in the user agreeing to utilise a cloud provider or to look elsewhere. This domain will be able to give the user some peace of mind, as it looks at security of data storage.

3.2.6 Spam

Although spam (a result of unsolicited electronic mail) may not seem like it has anything to do with data privacy - it does. When a user allows their personal information to be collected by another party, that data is no longer fully in their own control. This domain looks at some of the requirements behind the sending of unsolicited electronic mail.

As an example, let's say a hacker gets hold of a company's client database, which includes email addresses, by using some sort of address harvesting software. The hacker then uses those addresses to send out a large amount of spam. The company,

in this case, should understand if this is legal or not, and if there are requirements around what kind of spam is allowed, and which countries have strong spam legislation.

At first thought it may not seem like a domain to be included in the WDPM, but it involves the use of personal information which the user may not, and probably did not, consent to.

Spam has been around for a long time and takes many forms, these may include emails such as a the classic Nigerian prince - needing money or the Viagra emails. Mostly these emails are unsolicited meaning the recipient has not consented to receiving them.

3.2.7 Interception of Data

This domain has become a substantial area of interest in the past few years, especially after Edward Snowden released the vital documents outlining how the US Government was spying on its citizens. There are certain circumstances where Government or police can intercept a client's data if there is a legitimate reason to do so. Where it is done with proper authority, and in the interest of public safety or the security of the nation, then it should be acceptable. This domain looks at legislative requirements which are in place for this.

3.3 Domain Specifications

The domain specifications (referred to as specs from here) are the single most important ingredient to the WDPM. They list possible questions that a user may want to know. For example, a user may want to know what the legislation is,

across different countries, regarding what kind of security measures will be taken to ensure their data is kept safe while it is being stored.

Some of the initial specs came purely from brainstorming around current issues from news reports, articles or general questions from people. As research started on the specifications for NZ, other sections of the various Acts stood out as potential queries a user might have so these were rephrased into a generic spec and added to the list of the first draft. The same process happened for the other countries - if a section or a theme stood out across other countries it was added to the list.

Once the control domains had been grouped, after the first draft, and the second draft began, some of the specs were generalised so it wasn't as specific to one country but could then cover multiple countries.

3.4 Extra Additions

After a full second draft was completed, three additional features were added to the WDPM to give the user additional information and make it easier for quick reference.

The notes column was added to provide the user with additional information about the Acts mentioned, for the specification they were looking at. These notes just added a little more information for the user, for example, when the control specification states "Encryption techniques to store data" it adds a note for the user explaining "Although encryption is not specified, encryption may be used if it is seen as a reasonable protection method".

The second extra was the addition of the domain code column which helps the

user take notes and gives them a point for quick reference, without having to write down the whole control domain, domain specification and the relevant sections of the Acts.

The last and most important feature was making the documents in the legislative framework section hyperlinked. This was not in the original plan for the WDPM, but was a late addition after some external feedback. By the completion of the second full draft, the WDPM had hyperlinks to all of the legislation which had been used to find the relevant sections. The hyperlinks meant that the user could click on the hyperlinked document in the legislative framework control domain, and it would take them straight to the full document for them to use later. This reduces the time and potential money that a user may waste trawling the Internet, trying to find the relevant document. Some of these hyperlinks linked directly to the source, for example, NZ links directly to the Government legislation website, but for others like documents for China, these were copied and placed on the data privacy web server as a backup. Although this is not an ideal situation, it is the best way, at this stage to ensure these documents do not move from where they were found.

3.5 Chosen Countries

The WDPM originally started with the APAC region which included NZ, Australia, Malaysia, China and Singapore. These countries were chosen as they are some of the major cloud hosting countries within the APAC region. NZ was the first country to be chosen as the research is based in NZ, and the NZ legislation is

familiar.

It was then decided to look at comparisons between the EU and the US as these were two areas with a major stake in the cloud landscape, and also, because both regions would have to re-evaluate how they carried out data transfers, in the wake of the recent ruling of the Safe Harbour Agreement.

The EU countries - UK, France, Sweden, Germany, Poland and Estonia have been added as some of them make up the top cloud hosting countries, as well as giving a spread of different regions within the EU. A map of the chosen countries is shown in Figure 3.4.



Figure 3.4: This map shows the chosen countries

Chapter 4

Verification and Validation

This chapter will cover the verification and validation process for the WDPM as well as outlining the timeline and milestones for this research.

4.1 Verification

This section explains the verification process to verify the WDPM.

4.1.1 Vetting Process

As the WDPM offers legal guidance, specific people are required to verify the WDPM is correct. The people chosen to verify the WDPM need to be experts in the field of privacy law, but other law or privacy experts may (or will) be considered. These people require a good level of experience in dealing with privacy legislation or come recommended from someone with such experience. As easy as it is to use Google and search for “Privacy Expert” or “Privacy Lawyer” there is no way of telling their level of experience. Qualifications are one thing but the

WDPM needs the verification to come from people with the qualifications, and real world experience.

Each party selected to verify, will be looked at on a case by case basis to determine if they are suitable to contribute, and verify the work on the WDPM.

4.1.2 Verification by Privacy Experts

A range of privacy experts is needed in the verification process to ensure the WDPM is robust and up to date. These experts will come from a variety of backgrounds which includes lawyers who ideally have a background in privacy law or intellectual property law; however, the expertise of all lawyers could be utilised in verifying parts of the WDPM. Other experts will include policy makers dealing in privacy and cyber policies, such as Government Communications Security Bureau (GCSB) and National Cyber Policy Office (NCPO) in New Zealand. These government departments are key in New Zealand to developing new policies in the cyber and security space.

The privacy experts chosen to contribute to the WDPM have the potential to either directly add to a specific country or a range of countries, as their knowledge permits.

During verification there have been a number of experts who have contributed to the WDPM to verify the contents. Out of these experts, three were from NZ and one from the UK. Their contributions can be seen in the Verification From Experts Appendix. Katrine Evans [1] is at D.6, Neil Sanson [2] is at D.7, Michael Dizon [3] is at D.8 and Alan Shipman [4] is at D.9.

“ *The matrix is a great idea. These types of consolidations of local legislation, guidelines and standards are really useful. I was using one this morning, for instance, on data breach notification - a great quick reference guide. So go for it!*

”

Katrine Evans [1],

4.1.3 Verification Process

The method of getting the WDPM verified, is to approach legal professionals experienced in privacy law who can look over each of the various domains and check the following:

- Do the domains reflect legislative areas?
- Are the control specifications under each domain, suited to where it has been placed?
- Did the wording of the control specification make sense to the reader?
- Are the identified sections of legislation correct?

During the steps in the verification process outlined above, the party verifying the WDPM will have the ability to - make suggestions to the list of domains ensuring all areas of concern are covered, ensure the wording used to formulate the domain specifications is clear to the user, and to ensure that these domain specifications are placed in the correct domain. Any missing domain specifications or domains could be suggested, if the verifying party thought it was necessary to better cover a key area or to cover frequently asked questions they have from the public relating

to privacy.

The most vital step in the verification process is checking that the legislation and section(s) listed next to the domain specifications, refer to the correct sections in the correct legislation. Also, if a section has been missed or doesn't actually apply, the party verifying can suggest the correct change to make.

A minimum acceptance for the WDPM is to have two separate parties to verify each country. Giving it two different views, is a starting point to remove any bias or other conflicting factors.

4.2 Validation

The validation process involves approaching industry partners to validate the WDPM. The difference between verification and validation is that the verification is done through privacy experts looking over the WDPM and ensuring it is giving the user correct information, whereas the validation step is done through utilising industry partners, where they are able to have a copy of the WDPM for internal use to see what kind of benefits it offers them.

Validation is an important step in making the WDPM successful. Once validated, it shows other potential users the WDPM does everything it is supposed to do, and also shows them it will make their life easier if they use it. The business carrying out validation has the opportunity to give their feedback on ease of usage and quality of information sought. This feedback can then be used to make changes or, to show other users it is a helpful tool.

The validation comes from the feedback given by the business validating it. Validation will be measured as follows:

- Did using the WDPM save the business money in labour costs by decreasing time taken by an employee to research certain legislation?
- Did using the WDPM save the business money when it came to getting further legal advice?
- Did the control specifications in the WDPM cover the questions the business needed answers to?
- Was the WDPM user-friendly?

The main point to be validated is the potential cost savings for a business, from using the WDPM. If the business saves a total of 20 hours by using the WDPM that shows a spare 20 hours they could have spent somewhere else in the business. One of the companies approached for the validation was Gallagher, a Hamilton based company that is a “global leader in the innovation, manufacture and marketing of animal management, security, fuel systems and contract manufacturing solutions”. [55] Gallagher has offices in ten countries and is currently looking at expanding into some markets. The WDPM will be validated by Gallagher when they are ready to start looking into the expansion.

“The Waikato Data Privacy Matrix will be a very useful resource for us as we navigate the privacy requirements of the various regions we do business in. This is all research we were planning to do ourselves so the matrix will save us many weeks of time and help us get new products to international markets faster.”

Andrew Scothern [56], *Software Development Manager for
Gallagher Research and Development*

4.3 Verification Timeline

Due to the large number of experts needed in the verification step of the WDPM, verification started early on in the research. Once the first draft was completed in March 2016, contact was made with John Edwards - the New Zealand Privacy Commissioner. There were a few goals for contacting the Office of the Privacy Commissioner (OPC), first was to seek verification by experts in the office, second to get feedback on the WDPM and third to get other external contacts within New Zealand or overseas counterparts.

In April 2016 as a result of email correspondence with the OPC, contact was made with Katrine Evans from a law firm in Wellington. As a result, Katrine contributed to the WDPM with expert feedback around clarifications of control specifications and advice on sections which had been identified for the NZ column.

In April contact was made with the office of the Government Chief Privacy Officer of New Zealand. Initial response was positive but they were unable to give advice. After the second version was completed in June 2016, which included all 12 countries', contact was made to each of the countries data protection authorities to see if they were able to help verify the WDPM or pass it along to someone within that country who could help. This step was important to the research but came with a disappointing outcome in which none of the contacted authorities were able to offer any assistance.

One of the benefits of the WDPM being part of the research for the STRATUS project, was that it allowed us access to the industry advisory group. Gallagher was one of these members and as a result was interested in knowing more about how the WDPM could be beneficial to their business. After meeting with Gallagher and presenting WDPM they were excited to use the WDPM as they were about to expand into a new country and thought the WDPM would be a great help to their business. This would give the WDPM some validation in a real world scenario. Due to other factors Gallagher have not had a chance to use the WDPM yet. Correspondence with the OPC had continued, and in July 2016 the final version was completed and presented to the NZ Privacy Commissioner - John Edwards. The outcome was positive and some feedback was given at the time of the presentation and the following month further contributions were received from his team. The International Organization for Standardization (ISO) SC27 meetings were held in Abu Dhabi in October 2016. These meetings run over the course of a week and delegates who attend are involved in the Information and Communications Technology (ICT) and security and privacy areas. These meetings provided the opportunity to engage with IT, privacy and legal professionals, representing over 100 member countries, who would have interest in the research. INTERPOL in Singapore was approached for assistance with the WDPM as they have access to 190 member countries. It was hoped they would be able to use international connections to help with verification and validation in other countries. The Singapore Personal Data Protection Commission (PDPC) was also contacted with similar goals in mind as with the OPC in NZ. Again interest was shown but no further outcome or input has eventuated. The Asian Privacy Scholars Network is a network of privacy experts. The research

on the WDPM was presented at a conference in Auckland in December 2016. The conference also provided an opportunity to again engage with privacy professionals who had a variety of backgrounds and were from different countries around the APAC region. The timeline can be seen in Figure 4.1.

4.3.1 Milestones

The timeline has a four major milestones:

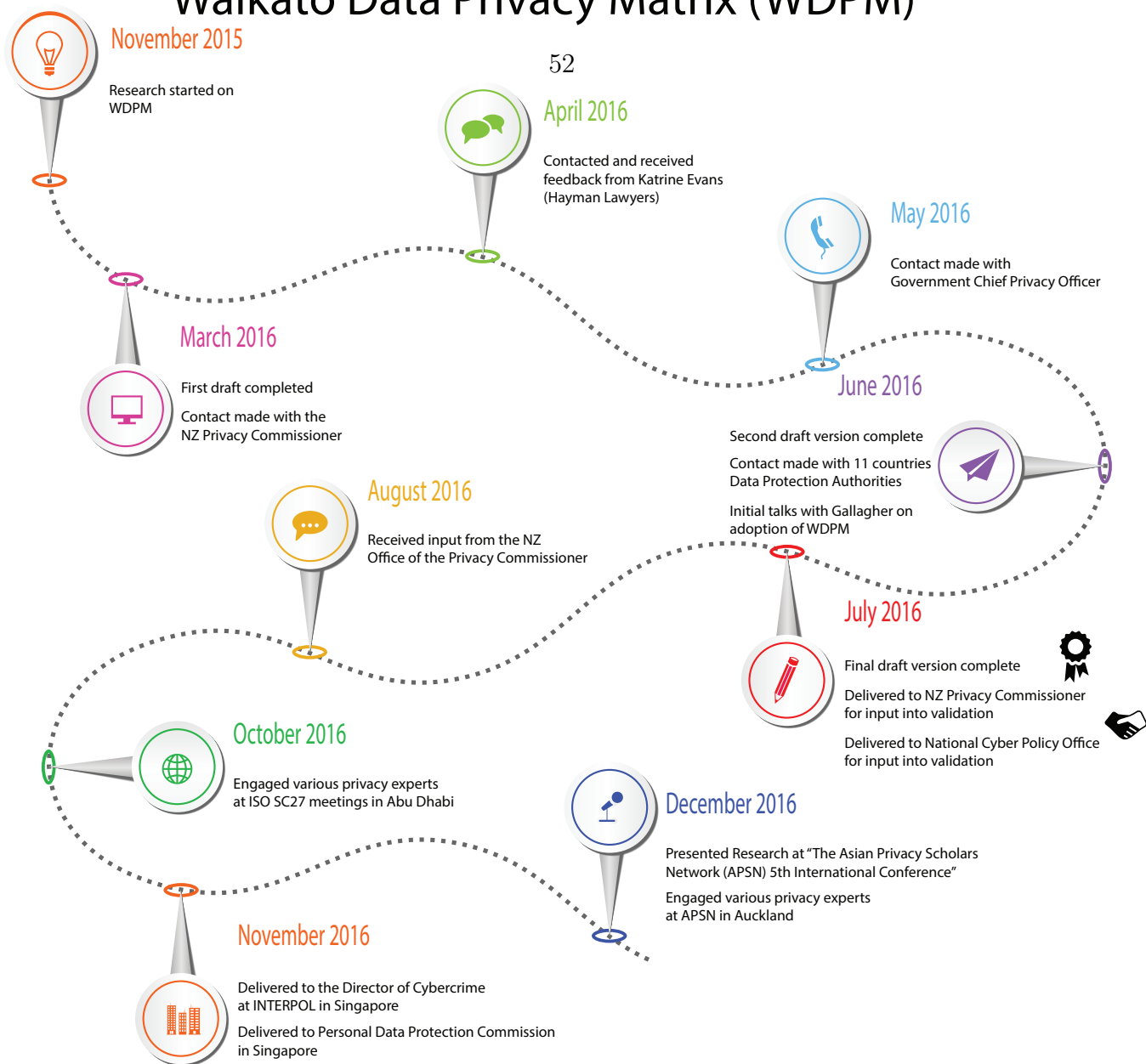
- Complete final product of WDPM
- Company validation
- Government Departments are involved
- Verified by at least two experts in each country

Two out of the four milestones were completed in July 2016. The first milestone was reached after the third version of the WDPM was finished. This allowed for progression for the rest of the milestones. Without a completed product, the remaining WDPM milestones would not have been possible.

The second milestone is still in progress, as mentioned previously in Sections 4.2 and 4.3 Gallagher was engaged as they were interested in using the WDPM to help their company expansion to other regions. However, this expansion has not yet happened, and as a result, this milestone is still in progress.

The third milestone was an important step for the WDPM and was successfully completed in July 2016 when two NZ government agencies were involved. The OPC and NCPO were both consulted, and a contribution was later made by the OPC. There is no hard stop for this milestone, in November 2016 the PDPC in

Timeline and Milestones of the Waikato Data Privacy Matrix (WDPM)



Milestones

	Complete final product of WDPM	Completed July 2016
	Company validation	In Progress
	Government Departments are involved	Completed July 2016
	Verified by at least 2 experts in each country	In Progress

Figure 4.1: Timeline and Milestones of Waikato Data Privacy Matrix

Singapore was also met with.

The last milestone is also still in progress. This milestone was to have at least two experts from each of the countries on the WDPM verify the WDPM. Although throughout this research there have been many experts engaged from these countries, this milestone is also an ongoing task.

All of these milestones have not yet been completed due to resource constraints, but they have helped contribute to the rigorous process this research and the WDPM have been through.

Chapter 5

Discussion of Results

This chapter will discuss the results of the research and some of the difficulties encountered while researching data privacy laws.

5.1 Expert Feedback

Throughout this research many individuals have been engaged to provide input or feedback. Everyone who has been exposed to this research has had positive comments to make, and this has helped to encourage the research and prove its importance and value. One of the first people to contribute to the WDPM was Katrine Evans who said this was a great idea. [1]. During the ISO meeting in Abu Dhabi, Eric Hibbard was approached, and he gave some great advice for further research.

“ As IT and OT intrude more into our lives and communities, data privacy becomes a very real concern and the regulatory response

varies wildly from jurisdiction to jurisdiction. The Data Privacy Matrix is a practical tool that helps individuals and organizations understand their rights and obligations as data traverses various jurisdictions with very different data protection requirements.

”

Eric Hibbard [57], *CISSP-ISSAP, ISSEP, ISSMP, CISA, CCSP, CTO Security Privacy, Hitachi Data Systems*

Also approached was Joanne Knight who was also able to help with the WDPM by introducing contacts she had in some of the other countries. One of these contacts was Alan Shipman from the UK who was able to contribute to the WDPM.

“ *The Waikato Data Privacy Matrix would provide a valuable resource for organisations providing services and individuals consuming them, where they occur on a transnational or global scale. Understanding what exists, what doesn't and ultimately how they can be aligned will greatly contribute to the protection of individuals' privacy.*

”

Joanne Knight [58],

Another professional approached at the ISO meeting was Tuukka Haarni, another privacy professional based in Finland who is a lead auditor for Inspecta [59].

“ *Rapid development of cloud computing and the commodification of personal data has greatly increased the need for frameworks and standards helping cloud providers and customers alike to have an*

understanding and controls on the protection of personally identifiable information (PII). As the data has gone global but the legislation mainly hasn't, there is a true need for tools like the Waikato Data Privacy Matrix.

”

Tuukka Haarni [60], *Lead Auditor, Inspecta (Finland)*

Towards the end of the research, the University of Waikato faculty of law gained a new asset in the form of Michael Dizon. Michael had previously worked for Baker & McKenzie, working on the 2013 edition of the Global Privacy Handbook (this resource was covered in section 2.7.4). Michael had valuable insight into this area and gave a great contribution shown in the Verification From Experts Appendix at D.8. As well as the contribution, Michael also made many useful comments which have added value to this research.

“(*The matrix provides a good overview and structure of the different aspects of data protection laws.*

The matrix makes it possible to compare and contrast different data protection laws around the world.

The added value of the matrix for lawyers is they can see what technical standards apply to a particular legal requirement and vice versa.

Data privacy is neither a purely technical nor a completely legal issue, it's a combination of both, the matrix addresses both areas.

Data protection laws are complex and use very technical and complex

language, by breaking these laws down into their component parts, the data privacy matrix makes these laws more accessible and understandable to the general public.

”

Michael Dizon [61], *Lecturer at Faculty of Law, University of Waikato*

5.2 Trends Observed

Over the course of this research and through the creation of the WDPM various trends have appeared. This section will discuss some of these important trends.

5.2.1 Security

When users look into using cloud services to store data, one constant concern is around security of the data. This may refer to data breaches, account hijacking or data loss to name a few [62].

One trend observed from this research is around data encryption. It is not specifically mentioned in legislation if encryption can be used in the processing or storing of data. This may be due to the rate in which technology grows and how legislation plays catchup to technology. Legislation attempts to be broad enough to cover a variety of issues. For encryption, legislatures have used similar wording to:

Privacy Act 1993 - Principle 5 (NZ)

Storage and security of personal information

An agency that holds personal information shall ensure—

- (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—
 - (i) loss; and
 - (ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
 - (iii) other misuse; and
- (b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

This is an example from the NZ Privacy Act 1993 that has similar suggestive wording which was noticed through the research. Although the wording does not specify encryption, it can be implied encryption would be a reasonable safeguard to secure data.

Encryption is a commonly accepted practice in all industries and is frequently used, but a minimum standard needs to be defined. For example, “All data which is being stored must be encrypted with a minimum standard of AES-128”.

5.2.2 Gaps

The WDPM is not necessarily just for users of cloud or web services, but it also has the potential to be used by governments to identify gaps within their own legal system.

Figure 5.1 shows an example of the WDPM “Pre-Collection Process” control domain and five control specifications. The first entry, “‘Sensitive Information’,

Control Domain	Domain Code	Control Specification	New Zealand Document name	Australia Document name	China Document name	United Kingdom Document name
Pre Collection Process	PCP-02	"Sensitive Information" is defined which gives examples and a clear outline		• Privacy Act 1988 Section 6	• PIP Section 3.7	• Data Protection Act 1998 Section 2
Pre Collection Process	PCP-03	Other types of information are defined that is viewed differently to personal or sensitive information			• PIP Section 3.8	
Pre Collection Process	PCP-04	Consent is required from the individual involved	• Privacy Act 1993 Schedule 5A	• Privacy Act 1988 Schedule 1, Principle 2	• PIP Section 4.2 d • SNIP Article 2 • Consumer Rights and Interests Article 29	• Data Protection Act 1998 Schedule 2 • CIB Article 5 (d)
Pre Collection Process	PCP-05	Type of consent required is either explicit or implicit		• Privacy Act 1988 Section 6		• Data Protection Act 1998 Schedule 3
Pre Collection Process	PCP-06	Consent needs to be written or verbal				
Pre Collection Process	PCP-07	Level of consent different for different age groups				

GAPS

Figure 5.1: Example of gaps

is defined giving examples and a clear outline”. The example shows Australia, China and the UK all have legislation in place where this definition can be found; however, NZ does not define sensitive information in legislation. This is a good example of where the NZ Government may want to include this definition in an upcoming amendment that would then align them with other countries.

Also in Figure 5.1 there are two control specification highlighted in yellow, one for “Level of consent different for different age groups” and the other for “Consent needs to be written or verbal”. There are no countries in the example which have this outlined in legislation for these (this maybe outlined in legislation for finance and health data but that is outside the scope of this research).

One example domain specification relates to what happens to a user’s data if the cloud provider or data centre is sold or closes down. Some companies have internal policies around this, but so far the WDPM shows a gap across all of the countries included in the WDPM.

This gap would assist governments, when drafting new Bills or amending existing Acts, to align with other countries that are included in the WDPM which could ultimately make all countries employ very similar legislation. By ensuring all countries have similar data privacy legislation, it means everyone would know what to expect, no matter where their data is being stored or processed, and every country would have the same procedures in place for retrieval, destruction and access.

The WDPM also provides other specifications that are being debated and discussed throughout the world. One example of this, is the GDPR due to come into force in the EU in March 2018. Understanding this Regulation allows users

and governments to ‘watch this space’ as it could mean potentially big changes, depending on where the user or government is located.

5.2.3 Upcoming Global Trends

This research has highlighted a growing concern for data privacy amongst countries, companies and individuals. This is due in part to advancement in IoT devices available on the market and how much data these devices can store and process. This trend does not seem like it will slow down anytime soon with other technologies emerging such as smart cities, autonomous vehicles and a range of other smart appliances.

One example of this trend being rectified is in the GDPR. This new regulation for the EU will allow for tighter regulations around data privacy which has previously been discussed in Section 2.5.2.1.

5.3 Challenges

5.3.1 Jurisdictional Differences

As jurisdictions are separated by geographical boundaries, the different jurisdictions have, over time, developed their own languages, cultures, moral and ethical beliefs. It is important, when looking at the legislation from another country, an individual is aware of these differences. This research had some challenges with languages and their translation, for the different countries involved in the WDPM.

Most jurisdictions make legislation freely accessible for anyone to look at. To view

NZ legislation, the user can go to <http://www.legislation.govt.nz> and navigate through the website to find the relevant Act. Australian legislation is similar and is at <https://www.legislation.gov.au>. China on the other hand does not have a freely available place to view legislation like other countries, instead a user can subscribe to this service. This is not an ideal situation for a user who only needs a one time look at legislation, or to search around different sites to find copies of the legislation.

5.3.1.1 Interpretations

A key part of any legislation is understanding the wording that is, firstly, used by the legislature when drafting, and secondly, what the legislature is actually trying to cover; this can be especially difficult as legislation is amended over time. For example, the NZ Security Intelligence Service Act was enacted in 1969, now 47 years later, technology has evolved, changing the security intelligence landscape. There have been at least seven amendments made to the Act. [63] But now it may be hard to interpret, as the original members of the legislature, who drafted the Act, would have had a different view of what the Act was supposed to accomplish; and the new legislature, making amendments, would have another view of what the Act should be doing, so parts of the Act may now mean something different.

When reading a section of legislation it is important to read it carefully obeying punctuation. There are two approaches when reading legislation - the literal approach and the purposive approach. The literal approach is where the reader looks primarily at the words of the legislation in order to construe its meaning. The purposive approach is where the reader looks at the sentence and the words

within the sentence, to see if the legislature had intended that section to cover more than just the literal meaning of the words.

A general user of cloud services may not have the technical knowledge, understanding of how cloud services work, or its terminology, but a user must be able to understand the risks involved with using cloud services.

5.3.1.2 Definitions

A definition explains what something means in general or in a specific context, and it can help to clear up any ambiguity. In legislation a word may have different definitions across different Acts. When a user of a cloud or web service wants to find out about another country's laws, regarding privacy of their data, they may find it hard and confusing to understand the terminology used or misinterpret how the legislation is intended to be used.

An example of how this wording can change between jurisdictions, is the term which is used to identify the person to whom personal data belongs. NZ refers to this as "individual concerned", Australia and Singapore refer to them as "individual", China refers to them as "Subject of personal information" and Malaysia and the EU use "data subject". Although it may seem obvious to some users that these have the same meaning, other users may find this confusing. The EU uses the term "processing" [25] which refers to any operation or set of operations performed on the data. Whereas in Asia Pacific countries, they specify in the section if it means delete, modify or destruction etc. These examples again show the necessity for a global alignment, and in this case not necessarily legislation itself but how the legislation is worded to limit this range of mixed terminology.

5.3.1.3 Language

One major challenge, which was faced in this research, was reading other countries' legislation when written in their official language. Also, trying to read and interpret legislation from non-English speaking countries became difficult, as not all of the countries in the WDPM published their legislation in English.

Legislation from China and EU countries, like France and Germany, was especially difficult as local websites were not in English which also meant their legislation was also not in English.

Two methods were utilised to assist with adding them to the WDPM - either relying on Google Translate to translate from the source language to English, or to search multiple websites for English versions.

The most effective way, was to search for English versions of the legislation, and once multiple copies had been acquired from different sources, they could be checked to make sure the wording matched up with each other, and then use Google Translate on one of the official ones, to double check the translation was correct.

5.3.1.4 Access to Legislation

This section will discuss how the challenges were faced regarding access to legislation, and the different legislative hierarchy which other countries have. These two issues were an important obstacle to understand before research could proceed further.

Access to legislation refers to two main areas - how easy the legislation is to locate, and how the legislation is laid out.

The first area, ease of locating legislation, showed that some of the countries were easy to find legislation for. For example, New Zealand, Australia, Singapore and the UK all have government websites where the legislation can be accessed. This makes it easy for people in these countries to find legislation. For other countries, there is no a central point to find legislation, and multiple third party websites had to be searched to find the legislation. Other countries have the legislation scattered across multiple websites, making it more time consuming to find relevant documents.

Another issue which arose, was trying to decipher how to actually read and navigate through the legislation. Some of the websites use PDF copies of the legislation or standard HTML. The New Zealand Privacy Act 1993, shown in Results Figures Appendix at Figure E.15, and the Australian Privacy Act 1988, shown in Results Figures Appendix at Figure E.14, are some of the easiest and well laid out legislation found. As shown in these two previously mentioned figures, their contents pages are hyperlinked to relevant parts of the legislation. For example when looking at the Privacy Act 1993 for the relevant section on the privacy principles, if the hyperlinked text “6 Information privacy principles” could be clicked on, linking straight to that section, it would save time.

Some of the legislation, once located, was hard to follow with the numbering that was used. Some countries simply use a default numbering system (1, 2, 3, 4 etc), which also includes using ‘Chapters’, ‘Articles’ ‘Parts’ and ‘Sections’ to differentiate areas of the legislation.

Legislation should be free to access and easily accessible, for the average person who does not have a background with law. At times, there were difficulties locating legislation for certain countries, and for other countries, difficulties following their

legislation.

The second area is the legislative hierarchy which refers to the order in which laws should be interpreted. Laws are interpreted from the highest form of law in a country to the lowest (usually a local by-law or regulation). Most countries follow a similar hierarchy where the constitution is the highest form of law followed by statutes enacted by Parliament (Acts). An example can be seen in Results Figures Appendix at Figure E.16. The US uses a different hierarchy which can be seen in Results Figures Appendix at Figure E.17

5.3.1.5 China

Access to legislation in China is not as straight forward as the other countries. The legislation is spread across multiple unofficial sources, or a few sites which seem legitimate but are difficult to navigate. One example of a legitimate website is pkulaw.cn [64]. This website allows access to various forms of legislation, regulations and decisions from the National People's Congress (NPC). This site does have an English portal but the user needs to have a subscription in order to download any of the documents. There are other sites which require a subscription to access legislation. There was no investigation done into the reasons for this or what the subscription was actually for.

The highest source of legal norms in the People's Republic of China is the "Constitution of the People's Republic of China". Following this are the Laws enacted by the NPC or the Standing Committee of the NPC then Administrative Regulations by the State Council. Most countries will have simple names, or at least easily

recognisable names, for legislation; for example, NZ and Australia both have a “Privacy Act” whereas China has a “National People’s Congress Standing Committee Decision Concerning Strengthening Network Information Protection”. Both are pieces of legislation that are in force but maybe slightly harder to recognise. A new user looking to store data in China may find it hard to locate such laws by not recognising the legal hierarchy and the naming conventions that are used.

5.3.1.6 United States

It was not difficult to find where the US legislation was located. It is spread across multiple government websites, however, the challenge came from finding relevant parts. US federal laws are codified into the United States Code (USC). The USC is made up of 52 ‘Titles’, each title is then divided into subtitles, parts, subparts, chapters, subchapters and more. Initially it took a long time to locate the relevant sections throughout the code until it was understood how to read the references from places such as Wikipedia. Google could then be used to search for an Act like the ‘Privacy Act 1974’, and a link followed to Wikipedia where it would explain the Act and show its code: ‘5 USC § 552a’ which brakes down to - Title five of the USC, Section 552a. Title five is easy enough to find but Section 552a is slightly more hidden. It is found at - Title 5 \implies PART I \implies CHAPTER 5 \implies SUBCHAPTER II \implies Sec 552a. Contrary to countries like NZ where a section is a small part of the overall Act, sec 552a in the USC is the whole Privacy Act 1974 which is around 16 pages of full text.

Once understood, this process to locate the relevant sections was easier and faster. This difficulty illustrates another reason why the WDPM is so useful.

5.3.1.7 Size of Acts

Legislation will vary in size depending on a few contributing factors which may be - how new the Act is, the scope of the Act and amendments made to the Act.

For example, when looking at the legislation in NZ, the Privacy Act 1993 has 156 pages, the Telecommunications Act 2001 has 249 pages and the Government Communications Security Bureau Act 2003 has only 32 pages. This was a similar situation, across all of the countries looked at, where the legislation ranged in size. The size was not a huge challenge as the the search function could be used to quickly look through the document for a variety of keywords, but this would be more of a challenge for someone with no legal background as terminology used may be not what one may expect.

5.3.1.8 No “Catch All” Legislation

Within the Asia Pacific, EU and US countries, there is no one size fits all legislation that covers all aspects of data privacy law. A country such as NZ has the Privacy Act 1993 [13] which has most of the legislation around data privacy, although there are additional parts that can be found in other Acts such as - the Telecommunications (Interception Capability and Security) Act 2013 [65], Unsolicited Electronic Messages Act 2007 [66] and Search and Surveillance Act 2012 [67]. This does not cover the amount of tortious and civil laws that may also be applicable to data privacy. Because there is such a wide variation between the relevant legislation, in relation to data privacy, it makes it difficult for a user to find which legislation may apply to themselves and their data, in jurisdictions outside of their residing country.

Technology is evolving at such a rapid rate that the legislative process within governments is not fast enough to keep up, so by the time a new Act has been passed, the technology may have evolved past a point where it is not relevant or it is possible to be bypassed. An example of this is with cyberbullying on social media sites such as Facebook. Facebook has been around for over a decade and in that time there have been many cases of cyberbullying, some of which have led to suicide. In 2015 NZ enacted the Harmful Digital Communications Act 2015 [68] which would have some impact on this sort of behaviour and make it a criminal offence. This is a perfect example of how such an intrusive act has taken the legislature a decade to address and the importance for an alignment of these global data privacy laws.

5.3.1.9 Verification and Validation

Verification of the WDPM has been exceptionally challenging. Many obstacles have come up in the verification process which have slowed down the rate of the project. As discussed in Chapter 4, verification is a critical step to the WDPM being successful. The verification process could be a time-intensive task, and as such some of the privacy experts who have been approached have asked for some sort of monetary payment, in exchange for giving up their time to contribute to the WDPM. This may seem a reasonable request in most circumstances, however, the WDPM is part of a project for a MCS thesis, and that highlights the next issue which was faced in the verification. Some of the privacy experts gave the impression that because of the WDPM University project, it would not be beneficial to collaborate on the project.

Verification of the WDPM is not a straight forward task that can be completed

in ten minutes, it needs experts to spend at least an hour of their time looking through their country and verifying it is correct; this process was explained in Section 4.1.3. Although the level of interest in the WDPM was very high, a large number of the experts felt they could not commit the time or resources towards verification, but many of them were impressed by the work done so far, on the WDPM.

One other challenge is that, because the WDPM is at the beginning of its life cycle, there is no real value attached to it yet.

Chapter 6

Conclusions

This thesis has looked at an effective way of comparing and aligning global data privacy legislation for users of cloud services. This research has led to the creation of the WDPM, a Rosetta Stone-like matrix for aligning global data privacy legislation from a number of different countries.

In Chapter 2, we looked at some of the recent history which has added fuel to the debates on online privacy. Although this thesis has only mentioned a few historical events and legal cases, these have had a considerable effect on moulding the data privacy landscape we are now seeing. In the same chapter, related work was explored and evaluated against the WDPM, which was then critically discussed at the end of the chapter, stating the key differences between existing work and the WDPM. Although this was not a ‘new idea’ per se, the novelty lies in the delivery of the information to the user. Instead of summarising the content of the legislation, the WDPM directs a user to the relevant legislation to help them discover the answer to their query. This information was delivered in the form of an Excel spread sheet which spans 42 A3 pages when printed, and can be seen in the

Conclusion Figures Appendix at Figure F.18. The advantage of the spreadsheet was that it allowed an easy way to compare jurisdictions by having it split into columns and rows; however, as this was built on from the original design, there is room for improvement.

As a result of the WDPM, there have been other results which were not intended at the start, and these have been discussed in Chapter 5, specifically how this work can be used by governments to identify gaps within their own legislation so they can align with other countries.

The final product of the WDPM is shown in the Conclusion Figures Appendix D.9. There are two examples here. One shows the whole WDPM which is not easy to read but has been included to show the size of the WDPM, and the second one shows a zoomed in view (this has been adapted to give an overview).

6.1 Future Work

The WDPM only focuses on general data privacy legislation at a federal level, meaning only legislation which covered the country as a whole was looked at. Due to the scope of the project only general data privacy was researched, this did not include legislation relating to health and finance. There were only twelve countries included in the WDPM as a start, the next step would be to add multiple other countries to create a more global and comprehensive alignment tool. The delivery for the WDPM is also an important step as the current form of the WDPM is a large Excel spreadsheet, but a web application will need to be introduced to make the user experience even better.

To ensure the WDPM is a truly global tool, a wider range of countries will also

need to be added.

6.1.1 Sectoral Additions

The WDPM focused on general data privacy legislation. This was due to the scope and time frame of the MCS. There are other areas where data privacy is important, and these were not covered here, but need to be included in the future. The two main areas which need to be looked at further are health/medical specific data and financial specific data. These two contrasting areas have various legislation in place, but unlike the Acts which cover general data privacy legislation, health specific and financial specific data are set out in their own various separate pieces of legislation.

These two areas play a large part in the world of data privacy as a user's medical or financial records contain huge amounts of personal or sensitive data, which if misused can be detrimental to an individual or a company.

6.1.2 Case Law

Laws are not only made through the government but also made through case law, or common law which is sometimes referred to as "judge made law". As the name suggests this law comes from the court system. When a case goes to court it is heard by a Judge, and the Judge will decide a ruling based on the interpretation of the legislation. The decision of the judge will create a precedent, which means, decisions from cases heard in a higher court are binding on lower courts in cases with similar facts that raise similar issues. The case law can then be followed in

some other jurisdictions. An example of this would be - if a case is heard in the Court of Appeal in NZ where the case involves the facts 'X', 'Y' and 'Z', and if a case is heard in a lower court like a District Court, where the case is similar and the facts presented are 'X', 'Y' and 'Z' then the case law can be used to decide the case.

An example can also be seen in Appendix E at figure F.19. In this example Case 1 sets a precedent in the Court of Appeal for a case where the facts 'X', 'Y' and 'Z' are present. This precedent could be applied to Case 2 as the facts are the same and it is in a lower court. Although the facts are the same in Case 4 it is a higher court so it is not binding, however the higher court may still choose to follow the precedent set by the lower court. Case 3 is in a lower court but only two of the three facts are the same so it would not apply to this case.

Including case law into the WDPM would give the user a better idea of how the courts are interpreting a specific section of legislation. Case law is a significant part of the legal system in the US and many of their laws are common law. However, including case law would be a substantial task to undertake due to the large amount of case law that exists.

6.1.3 State Legislation

The WDPM has only focused on federal legislation which looks at the top level legislation in each country. There are many countries which are also made up of various states and these states enact their own law to dictate how their state operates and exists in parallel with the federal legislation.

The US, Australia and Germany are just some countries that have state law. Figure E.17 in Appendix E shows how the US legislative hierarchy is laid out, indicating that State legislation makes up a big part of the US legal system. Within the US each state creates their own constitution, governmental structure, legal codes, and judiciary. These may sometimes conflict with the federal system. [69]

Adding state legislation to the WDPM will be a huge task, but will be extremely beneficial for users and governments to see how their data will be affected in each of these states. Although federal legislation will trump state legislation, it is still vital that users understand these different areas.

6.1.4 Data Privacy Foundation Inc.

To help to complete the future work and promote the WDPM and data privacy, the Data Privacy Foundation Inc. is being setup. The foundation has the following vision:

- (a) To assist in achieving global alignment of data privacy laws by identifying gaps and shortfalls in country and regional laws and legal systems, thereby ensuring full legal protection of data.
- (b) To establish the premier, knowledge based, definitive global authority on data privacy.
- (c) To provide knowledge, tools, training, consultancy and events to assure data privacy across the globe.
- (d) To establish, build, and sustain data privacy knowledge databases by harnessing collaborative, open source, scalable

contributions and technologies.

(e) To facilitate delivery of data privacy at a level not achievable or limited by any one organisation or country.

The Foundation will help to create a comprehensive and robust global alignment tool for all types of data privacy legislation mentioned in Future Work section. There is a lot of work to be done to include these extra additions but this is a crucial development to create a truly global tool, and the benefit of having the Foundation will help to extend the reach of this research.

By having access to federal and state legislation combined with case law, users and governments have a tool which gives them extensive information and direction to data privacy legislation around the globe.

Chapter 7

List of Publications

Craig Scoon and Ryan K L Ko, “The Data Privacy Matrix Project: Towards a Global Alignment of Data Privacy Laws”, The 1st IEEE International Workshop on Security and Privacy in Advanced Persistent Threat (SPAPT 2016), held in conjunction with 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16), Tianjin, China, 23-26 August, 2016 [70]

Craig Scoon and Ryan K L Ko, “Data Privacy Matrix,” Chapter in “Data Security in Cloud Computing”, Eds. Vimal Kumar, Ryan K L Ko & Sivadon Chaisiri, Institution of Engineering and Technology, United Kingdom, 2017 (In submission) [71]

References

- [1] K. Evans, Personal Communication, 29 May 2016.
- [2] N. Sanson, Personal Communication, 23 August 2016.
- [3] M. Dizon, Personal Communication, 12 January 2017.
- [4] A. Shipman, Personal Communication, 12 December 2016.
- [5] Wikimedia Commons. (2013) Legislative procedure uk. (Last Accessed on 13 September 2016). [Online]. Available: [https://en.wikipedia.org/wiki/Bill_\(law\)#/media/File:Legislative_procedure_uk.svg](https://en.wikipedia.org/wiki/Bill_(law)#/media/File:Legislative_procedure_uk.svg)
- [6] University of Portsmouth, “Legislative powers of the European Parliament,” 2013, (Last Accessed on 03 September 2016). [Online]. Available: <http://hum.port.ac.uk/europeanstudieshub/learning/module-1-understanding-eu-institutions/the-european-parliament/legislative-powers-of-the-european-parliament/>
- [7] Office of the Clerk of the House of Representatives, “The legislative process,” March 2014, (Last Accessed on 01 September 2016). [Online]. Available: <https://www.parliament.nz/media/2161/parliament-brief-the-legislative-process.pdf>
- [8] “Data Protection Laws of the World,” (Last Accessed on 30 August 2016). [Online]. Available: <https://www.dlapiperdataprotection.com/#handbook/world-map-section>
- [9] “Global Heat Map,” (Last Accessed on 30 August 2016). [Online]. Available: <http://heatmap.forrestertools.com/>

- [10] Jeff Rohlmeier, “International Data Protection Legislation Matrix,” (Last Accessed on 30 August 2016). [Online]. Available: <http://web.ita.doc.gov/ITI/itiHome.nsf/51a29d31d11b7ebd85256cc600599b80/4947d6deb021a96485256d48006403af?OpenDocument>
- [11] Baker McKenzie, “Global Privacy Handbook,” 2016, (Last Accessed on 30 August 2016). [Online]. Available: <http://globalprivacymatrix.bakermckenzie.com/>
- [12] “Privacy Act 1988,” 1988, (Last Accessed on 16 December 2016). [Online]. Available: <https://www.legislation.gov.au/Details/C2016C00979>
- [13] “Privacy Act 1993,” 1993, (Last Accessed on 04 April 2016). [Online]. Available: <http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html>
- [14] Vic (J.R.) Winkler, “Cloud Computing: Privacy, confidentiality and the cloud,” June 2013, (Last Accessed on 24 October 2016). [Online]. Available: <https://technet.microsoft.com/en-us/library/dn235775.aspx>
- [15] I. Georgieva, “The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR,” *Utrecht J. Int’l & Eur. L.*, vol. 31, p. 104, February 27 2015, (Last Accessed on 24 October 2016). [Online]. Available: www.utrechtjournal.org/articles/10.5334/ujel.cr/
- [16] N. Arce, “Effect Of NSA Spying On US Tech Industry: \$35 Billion? No. Way More,” June 10 2015, (Last Accessed on 22 July 2016). [Online]. Available: <http://www.techtimes.com/articles/59316/20150610/effect-of-nsa-spying-on-us-tech-industry-35-billion-no-way-more.htm>
- [17] K. L. Lueth, “Why the Internet of Things is called Internet of Things: Definition, history, disambiguation,” December 19 2014, (Last Accessed on 24 October 2016). [Online]. Available: <https://iot-analytics.com/internet-of-things-definition/>

- [18] L. Columbus, “Roundup Of Cloud Computing Forecasts And Market Estimates, 2016,” March 13 2016, (Last Accessed on 24 October 2016). [Online]. Available: <http://www.forbes.com/sites/louiscolombus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#5557f3c574b0>
- [19] M. Cartwright, “Rosetta Stone,” January 03 2014, (Last Accessed on 16 December 2016). [Online]. Available: http://www.ancient.eu/Rosetta_Stone/
- [20] “2013 BSA Global Cloud Computing Scorecard,” 2013, (Last Accessed on 30 May 2016). [Online]. Available: <http://cloudscorecard.bsa.org/2013/countries.html>
- [21] “STRATUS,” (Last Accessed on 24 October 2016). [Online]. Available: <https://stratus.org.nz/>
- [22] Department of the Prime Minister and Cabinet (New Zealand), “National Plan to Address Cybercrime,” December 10 2015, (Last Accessed on 24 August 2016). [Online]. Available: <http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdf>
- [23] Department of the Prime Minister and Cabinet (Australia), “Australia’s Cyber Security Strategy,” April 21 2016, (Last Accessed on 24 August 2016). [Online]. Available: <https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf>
- [24] S. Nicholas, “Surviving and thriving with your new business,” September 22 2015, (Last Accessed on 24 August 2016). [Online]. Available: <http://www.stuff.co.nz/business/better-business/72295224/Surviving-and-thriving-with-your-new-business>
- [25] “EU Data Protection Directive,” 1995, (Last Accessed on 06 April 2016). [Online]. Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en>

- [26] “Questions and Answers on the EU-US data protection Umbrella agreement,” September 08 2015, (Last Accessed on 03 April 2016). [Online]. Available: http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm
- [27] “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” September 23 1980, (Last Accessed on 03 April 2016). [Online]. Available: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>
- [28] G. Maldoff, “We read Privacy Shield so you don’t have to,” March 07 2016, (Last Accessed on 04 April 2016). [Online]. Available: <https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to>
- [29] E. Commission, “EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield,” February 02 2016, (Last Accessed on 24 August 2016). [Online]. Available: http://europa.eu/rapid/press-release_IP-16-216_en.htm
- [30] S. Colclasure, “The EU Privacy Shield one week in: A privacy exec’s perspective,” August 10 2016, (Last Accessed on 24 August 2016). [Online]. Available: <http://venturebeat.com/2016/08/10/the-eu-privacy-shield-one-week-in-a-privacy-execs-perspective/>
- [31] “The legal system of the european union.”
- [32] Council of European Union, “Directive 2009/136/EC,” 2009, (Last Accessed on 3 August 2016). [Online]. Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=EN>
- [33] —, “Directive 2006/24/EC,” 2006, (Last Accessed on 3 August 2016). [Online]. Available: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>
- [34] EUGDPR.org, “GDPR Key Changes,” (Last Accessed on 13 December 2016). [Online]. Available: <http://www.eugdpr.org/key-changes.html>

- [35] A. Macrae, “GDPR – The Good, the Bad and the Ugly,” February 23 2016, (Last Accessed on 12 January 2017). [Online]. Available: <https://www.tripwire.com/state-of-security/security-awareness/gdpr-the-good-the-bad-and-the-ugly/>
- [36] A. Olshanskaya, “Why the GDPR is good for business,” December 15 2016, (Last Accessed on 12 January 2017). [Online]. Available: <https://iapp.org/news/a/why-the-gdpr-is-good-for-businesses/>
- [37] S. M. Lisa Mays, “The Schrems Decision: How the End of Safe Harbor Affects Your FCPA Compliance Plan,” November 12 2015, (Last Accessed on 27 August 2016). [Online]. Available: <http://www.globaltradelawblog.com/2015/11/12/the-schrems-decision-how-the-end-of-safe-harbor-affects-your-fcpa-compliance-plan/>
- [38] “The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid,” October 6 2015, (Last Accessed on 04 April 2016). [Online]. Available: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>
- [39] F. Coudert, “Schrems Vs. Data Protection Commissioner: a Slap on the Wrist for the Commission and New Powers for Data Protection Authorities,” October 15 2015, (Last Accessed on 27 August 2016). [Online]. Available: <http://europeanlawblog.eu/?p=2931>
- [40] L. Laudati, “Summaries of Eu Court Decisions Relating to Data Protection 2000-2015,” January 28 2016, (Last Accessed on 27 August 2016). [Online]. Available: https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf
- [41] “Google Spain v AEPD and Mario Costeja González (C131/12),” 2014, (Last Accessed on 06 April 2016). [Online]. Available: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065
- [42] “Factsheet on the “Right to be forgotten” ruling,” (Last Accessed on 07 April 2016). [Online]. Available: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

- [43] E. Ortiz, “San Bernardino Shooting: Timeline of How the Rampage Unfolded,” December 03 2015, (Last Accessed on 27 August 2016). [Online]. Available: <http://www.nbcnews.com/storyline/san-bernardino-shooting/san-bernardino-shooting-timeline-how-rampage-unfolded-n473501>
- [44] T. Cook, “Answers to your questions about Apple and security,” February 16 2016, (Last Accessed on 29 August 2016). [Online]. Available: <https://www.apple.com/customer-letter/answers/>
- [45] A. Kharpal, “Apple vs FBI: All you need to know,” March 29 2016, (Last Accessed on 29 August 2016). [Online]. Available: <http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html>
- [46] K. Zetter, “Apple’s FBI Battle Is Complicated. Here’s What’s Really Going On,” February 18 2016, (Last Accessed on 29 August 2016). [Online]. Available: <https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/>
- [47] “Right to be Forgotten FAQs,” 2014, (Last Accessed on 26 July 2016). [Online]. Available: <https://forget.me/faq>
- [48] D. Sullivan, “How Google’s New “Right To Be Forgotten” Form Works: An Explainer,” May 30 2014, (Last Accessed on 28 July 2016). [Online]. Available: <http://searchengineland.com/google-right-to-be-forgotten-form-192837>
- [49] L. Clark, “Google’s ‘right to be forgotten’ response is ‘disappointingly clever’,” May 30 2014, (Last Accessed on 28 July 2016). [Online]. Available: <http://www.wired.co.uk/article/google-right-to-be-forgotten-form>
- [50] D. Sullivan, “Google To Remove Right-To-Be-Forgotten Links Worldwide, For Searchers In European Countries,” February 10 2016, (Last Accessed on 28 July 2016). [Online]. Available: <http://searchengineland.com/google-to-remove-all-right-to-be-forgotten-links-from-european-index-242235>
- [51] “The right to be forgotten - between expectations and practice,” November 20 2012, (Last Accessed on 28 July 2016). [Online]. Available: <https://www.enisa.europa.eu/publications/the-right-to-be-forgotten>

- [52] Heidi Shey et al., “Privacy, Data Protection, And Cross-Border Data Transfer Trends In Asia Pacific,” March 04 2005, (Last Accessed on 30 August 2016). [Online]. Available: <https://www.forrester.com/report/Privacy+Data+Protection+And+CrossBorder+Data+Transfer+Trends+In+Asia+Pacific/-/E-RES131051#figure2>
- [53] Baker McKenzie, “Firm Facts,” 2016, (Last Accessed on 30 August 2016). [Online]. Available: <http://www.bakermckenzie.com/-/media/files/about-us/firm-facts-final.pdf?la=en>
- [54] Dropbox, “Dropbox.com,” (Last Accessed on 03 September 2016). [Online]. Available: <https://www.dropbox.com>
- [55] Gallagher, “About Us,” (Last Accessed on 18 January 2017). [Online]. Available: <https://www.gallagher.com/about-us/>
- [56] A. Scothern, Personal Communication, 20 January 2017.
- [57] E. Hibbard, Personal Communication, 20 January 2017.
- [58] J. Knight, Personal Communication, 20 January 2017.
- [59] “Inspecta.com,” (Last Accessed on 20 January 2017). [Online]. Available: <http://www.inspecta.com/>
- [60] T. Haarni, Personal Communication, 22 January 2017.
- [61] M. Dizon, Personal Communication, 20 January 2017.
- [62] Top Threats Working Group, Cloud Security Alliance. (February 2016) ‘The Treacherous Twelve’ Cloud Computing Top Threats in 2016. (Last Accessed on 18 January 2017). [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
- [63] “New Zealand Security Intelligence Service Act 1969,” 1969, (Last Accessed on 14 September 2016). [Online]. Available: <http://www.legislation.govt.nz/act/public/1969/0024/latest/versions.aspx?av=True>

- [64] “pkulaw.cn,” (Last Accessed on 13 October 2016). [Online]. Available: <http://www.pkulaw.cn/>
- [65] “Telecommunications (Interception Capability and Security) Act 2013,” 2013, (Last Accessed on 04 April 2016). [Online]. Available: <http://www.legislation.govt.nz/act/public/2013/0091/latest/DLM5177923.html#DLM5178025>
- [66] “Unsolicited Electronic Messages Act 2007,” 2007, (Last Accessed on 04 April 2016). [Online]. Available: <http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html>
- [67] “Search and Surveillance Act 2012,” 2012, (Last Accessed on 04 April 2016). [Online]. Available: <http://www.legislation.govt.nz/act/public/2012/0024/latest/DLM2136536.html>
- [68] “Harmful Digital Communications Act 2015,” 2015, (Last Accessed on 04 April 2016). [Online]. Available: <http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html>
- [69] D. D. LLC, “Federal vs. State Law,” December 03 2016, (Last Accessed on 15 December 2016). [Online]. Available: http://www.diffen.com/difference/Federal_Law_vs_State_Law
- [70] Craig Scoon and Ryan K L Ko, “The Data Privacy Matrix Project: Towards a Global Alignment of Data Privacy Laws,” 2016.
- [71] Craig Scoon and Ryan Ko, “Data Privacy Matrix,” in *Data Security in Cloud Computing*, Vimal Kumar, Ryan K L Ko & Sivadon Chaisiri, Ed. United Kingdom: Institution of Engineering and Technology, 2017, ch. 13.
- [72] “The History of Cloud Computing,” (Last Accessed on 27 August 2016). [Online]. Available: <http://www.eci.com/cloudforum/cloud-computing-history.html>
- [73] A. Mohamed, “A history of cloud computing,” (Last Accessed on 27 August 2016). [Online]. Available: <http://www.computerweekly.com/feature/A-history-of-cloud-computing>

- [74] Business Cloud News, “AWS, Google, Microsoft and IBM pull away from pack in race for cloud market share,” April 29 2016, (Last Accessed on 27 August 2016). [Online]. Available: <http://www.businesscloudnews.com/2016/04/29/aws-google-microsoft-and-ibm-pull-away-from-pack-in-race-for-cloud-market-share/>
- [75] J. Tsidulko, “Keeping Up With The Cloud: Top 5 Market-Share Leaders,” February 11 2016, (Last Accessed on 27 August 2016). [Online]. Available: <http://www.crn.com/slide-shows/cloud/300079669/keeping-up-with-the-cloud-top-5-market-share-leaders.htm/pgno/0/6>
- [76] K. Weins, “Cloud Computing Trends: 2016 State of the Cloud Survey,” February 09 2016, (Last Accessed on 06 April 2016). [Online]. Available: <http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey>
- [77] “Google Data Centres,” February 09 2016, (Last Accessed on 07 April 2016). [Online]. Available: <https://www.google.com/about/datacenters/inside/locations/index.html>
- [78] M. B. Kelly, “The US Now Thinks Snowden ‘Probably Downloaded’ 1.5 Million Documents That Haven’t Been Found,” June 06 2014, (Last Accessed on 22 July 2016). [Online]. Available: <http://www.businessinsider.com.au/clapper-says-snowden-took-less-than-they-thought-2014-6>
- [79] “Verizon - about us,” (Last Accessed on 12 July 2016). [Online]. Available: <http://www.verizon.com/about/our-company/history-timeline>
- [80] “Court order to spy on Verizon users is a 3-month renewal of ongoing practice: Feinstein,” June 06 2013, (Last Accessed on 22 July 2016). [Online]. Available: <http://nypost.com/2013/06/06/court-order-to-spy-on-verizon-users-is-a-3-month-renewal-of-ongoing-practice-feinstein/>
- [81] P. Szoldra, “SNOWDEN: Here’s Everything We’ve Learned In One Year Of Unprecedented Top-Secret Leaks,” June 07 2014, (Last Accessed on

- 22 July 2016). [Online]. Available: <http://www.businessinsider.com.au/snowden-leaks-timeline-2014-6?r=US&IR=T>
- [82] J. Schellhase, “After Two Years of Edward Snowden Revelations, What Have We Learned About NSA Spying?” May 06 2015, (Last Accessed on 22 July 2016). [Online]. Available: <http://all-that-is-interesting.com/snowden-revelations/3>
- [83] B. Dreyfuss and E. Dreyfuss, “What is the NSA’s PRISM program? (FAQ),” June 07 2015, (Last Accessed on 21 July 2016). [Online]. Available: <http://www.cnet.com/news/what-is-the-nsas-prism-program-faq/>
- [84] “PRISM Slides,” June 07 2015, (Last Accessed on 25 August 2016). [Online]. Available: <https://nsa.gov1.info/dni/prism.html>
- [85] T. Sottek and J. Kopstein, “Everything you need to know about PRISM,” July 17 2013, (Last Accessed on 03 April 2016). [Online]. Available: <http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>
- [86] Francoise Gilbert and Marie-Jose Van Der Heijden, *EU-U.S. Privacy Shield 2.0 Signed, Sealed and Delivered*. Bloomberg BNA - Privacy and Security Law Report, July 7 2016, iSSN 1538-3423 (Last Accessed on 24 August 2016). [Online]. Available: <https://www.bna.com/euus-privacy-shield-n57982076797/>

Appendix A

Related Background

A.1 Cloud Computing

Cloud computing started in 1999 when Salesforce became one of the first major companies to move into the cloud business. Salesforce started the concept of providing enterprise-level applications to any user providing they had Internet access. [72]

Amazon Web Services were launched in 2002 offering a suite of cloud-based services for customers, including storage and computation. In 2006 Amazon introduced its Elastic Compute Cloud (EC2) to the public. [73] A survey conducted by Synergy Research Group in 2016 found that Amazon controlled 31% of the cloud market share for the first quarter in 2016 [74]. This is the same as the result for this survey when conducted for 2015 fourth quarter, with Microsoft, IBM and Google coming in under Amazon. [75]

In January 2016 RightScale - an organisation deploying and managing applications in the cloud, conducted its annual State of the Cloud Survey of the latest cloud computing trends which focuses on cloud users and cloud buyers. There were 1,060 IT professionals who participated in the survey, and of these participants 95% were using cloud services [76]. To utilise cloud computing, it is essential to have multiple data centres located in different parts of the country or the world, to ensure lower latency for the customers using the cloud service. Google has many data servers scattered across the globe, but it is unclear the precise number of data centres that Google operates [77]. Although this is good for users who have their data stored in these places, it makes it difficult to know what laws apply to their data. Even if a user has data stored in the US their data may be subjected to different state laws

depending on which part of the country it is stored in. What makes matters more unclear is when a user has their data stored in multiple data centres in different parts of the world. Internet addresses are not physical addresses, which allows them to be easily spoofed, making it harder to locate where the data came from or showing the data is residing in an entirely different country. There is a clear need for policy makers to collaborate on these laws so there is a global alignment which does not produce any surprises for users of these services.

A.2 The NSA Leaks

In 2013 Edward Snowden, a former employee of defence contractor Booz Allen Hamilton at the NSA, released classified information relating to numerous global surveillance programs, many of which were run by the NSA and the Five Eyes Alliance. Snowden met with two reporters, in Hong Kong, from a British daily newspaper - The Guardian. Snowden revealed top secret classified information relating to the clandestine surveillance program known as PRISM, and other information about covert spying operations carried out by the US government on its citizens. It was originally thought that Snowden downloaded 1.5 million documents but only shared around 200,000 [78] with the two original journalists from The Guardian. However this has not been confirmed.

The leaked documents revealed how the Foreign Intelligence Surveillance Court (FISC) had ordered Verizon - an American telecommunications company - to hand over millions of customers' telephone records [79]. This was not so the NSA could pry into the content of these calls, but it did allow the NSA's computers to look through the millions of phone records for patterns or unusual types of behaviour.

[80] This practice had been going on for approximately seven years, on a three monthly renewal system.

The documents also revealed top-secret procedures that showed steps the NSA must take to target and collect data from “non-US. citizens” and how it must minimise data collected on its own US citizens. There were also documents relating to a program codenamed ‘EvilOlive’ [81] which collected and stored large amounts of Internet metadata from US citizens, including sender, recipient, and time stamp of email correspondences from Internet users. [82]

Since the leaks, the Information Technology and Innovation Foundation (ITIF), an industry-funded think tank that focuses on the intersection of technological innovation and public policy, estimated the leaks could cost cloud computing companies up to \$35 Billion in lost revenue. [16]

The fallout from this exposure forced countries that were using data centres in the US to open data centres in their own countries or look for other places to store data. Russia received this news and passed a new law which required all tech companies inside Russian borders to only use servers located within Russia. This is one way of not having to worry about a global alignment, but it is an extremely high cost for the companies to use backyard data centres. [16] It also forced users of cloud services to look into where their data was going to be stored or if it would be moved from the US centres to another part of the world where the laws were unknown to them.

A.3 PRISM

Documents released by Snowden revealed the surveillance program - PRISM, which was launched in 2007 after the enactment of the Foreign Intelligence Surveillance Act (FISA). Carried out by the NSA, PRISM collects stored Internet communications and uses data mining techniques to look for patterns of terrorism, or other potential criminal activity within the communications. The program is designed to collect and process “foreign intelligence” that passes through American servers at any point in the communication. [83] Much of the global communication travels through the US, at some stage, and this may be because it is cheaper to pass through the US than to take the most direct route. [84]

There were at least nine major US Internet companies participating in this program which included Microsoft in 2007, Yahoo in 2008, Google, Facebook and Paltalk in 2009, YouTube in 2010, AOL and Skype in 2011, and Apple in 2012 [85]. The partnerships with these companies allowed access to ten types of content including audio, video, photographs, e-mails, documents and connection logs. [84] The basic idea behind the program was for the NSA to have the ability to request data on specific persons of interest. Permission was given by the FISC, a special federal court setup by the FISA. There are still questions about the operation of the FISC and if its actions are in breach of the US constitution.

A.4 New Zealand Cyber Security Strategy

Cyber resilience involves detection, protection and recovery from cyber incidents, and looking to create action plans for disaster recovery from cyber incidents.

Cyber capability refers to educating the public and providing them with the necessary tools they may need. It focuses on individuals, businesses, government departments, and organisations to build better cyber security capabilities and awareness. The success of this goal will allow all levels of New Zealanders to have the knowledge and tools available to protect themselves against a cyber threat. This should also have the potential to increase the skills in the cyber security industry, allowing businesses and organisations to have the technical staff to support the rest of their IT team.

Addressing cybercrime looks at prevention of cyber crime, but also has an extra component, in the “National Plan to Address Cybercrime” which identifies cybercrime issues and challenges and ways they can be addressed. Most of this is from awareness, so the public can learn to help themselves.

International cooperation is the last goal which is vital to mitigating risk within cybercrime. This looks at building international partnerships within the APAC region.

A.5 Privacy Shield

The new and approved version of the Privacy Shield contains numerous clarifications for the privacy principles.

The first relates to data integrity and purpose limitation, which clarifies the purpose of data usage and that it is reliable for its intended use; meaning it must be up to date and complete.

The choice principle allows the data subject to opt-out if their data will be disclosed to a third party or used for a different purpose, and clarifies the use for direct

marketing.

The principle on accountability for onwards transfers, clarifies the obligation to all parties involved, of the processing of data being transferred to ensure the same level of protection despite the location of that party.

The access principle is probably the most important principle in the Privacy Shield. It allows a data subject to query an organisation if they are processing any personal data related to them, which the organisation needs to respond to, in a reasonable time. Although, the problem here is what constitutes reasonable. This is a subjective interpretation of the word so this may cause some problems in the future. It also allows for the data subject to correct, amend, or delete personal data that is inaccurate or has been processed in violation of the Principles. This aligns with the EU directives and regulations.

The principle on Recourse, Enforcement and Liability clarifies how complaints are handled, and sets out eight levels of redress that must be handled in a specific order, which would be used for EU citizens if their complaint is not resolved to their satisfaction. [86]

Since the Privacy Shield was built upon parts of the Safe Harbour Agreement, companies still need to self-certify. It has the extra principle components, meaning citizens from the EU are protected better than before, and there is more transparency in this agreement.

Appendix B

Background Chapter Figures

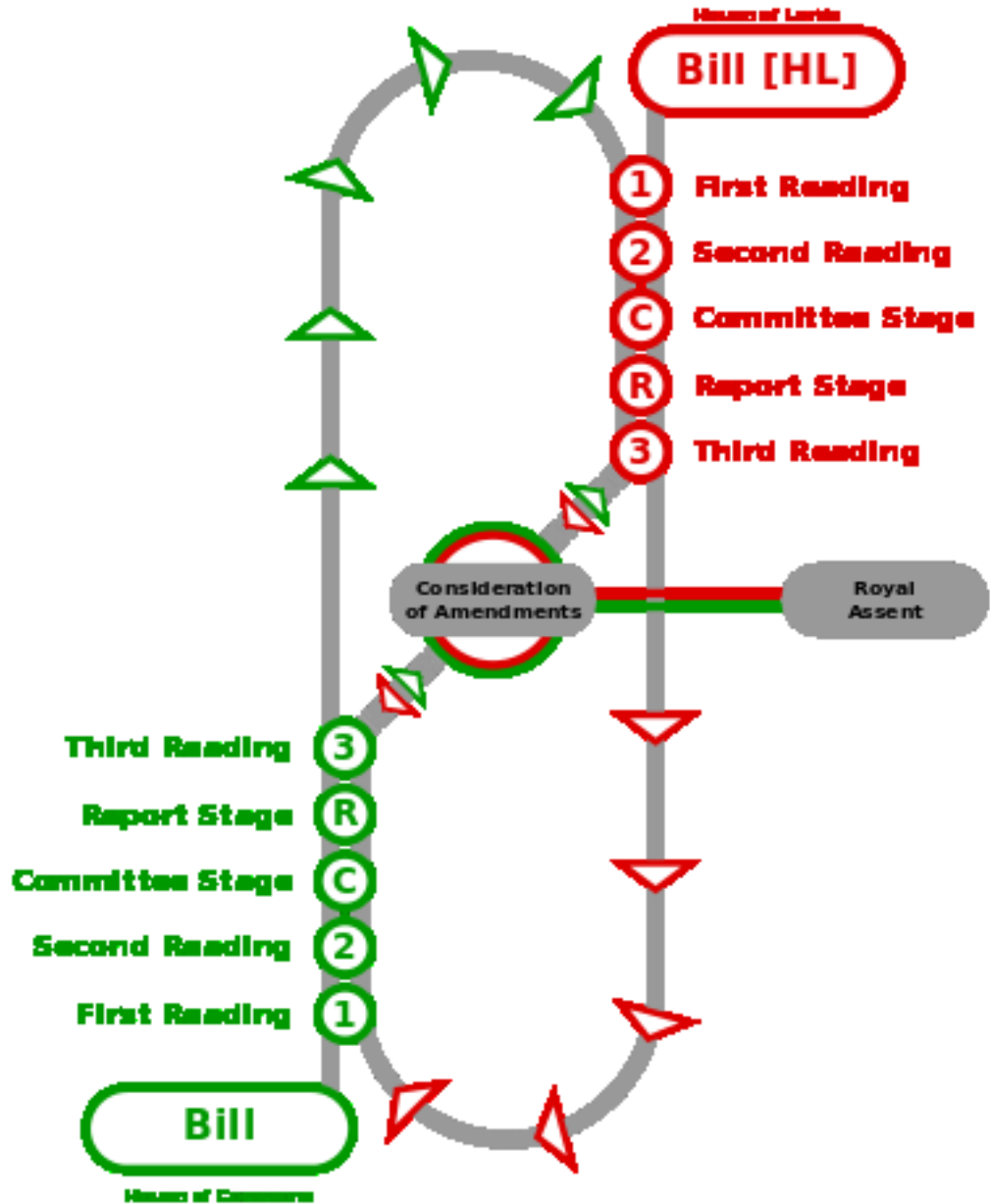


Figure B.1: A general outline of the stages a Bill will pass through in the legislative process within commonwealth countries [5].

United States Federal Legislative Process

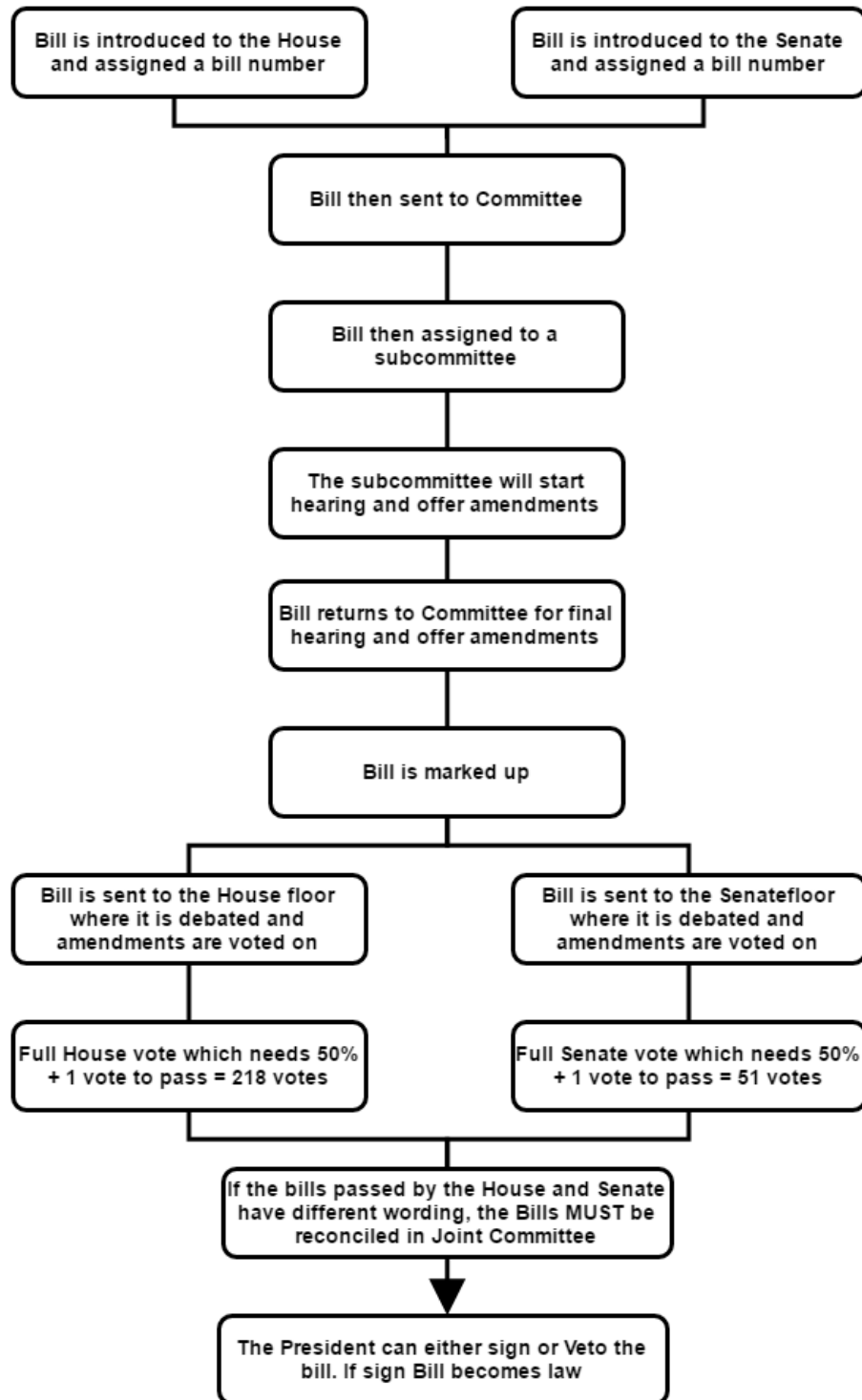


Figure B.2: Flowchart of the Federal legislative process in the US

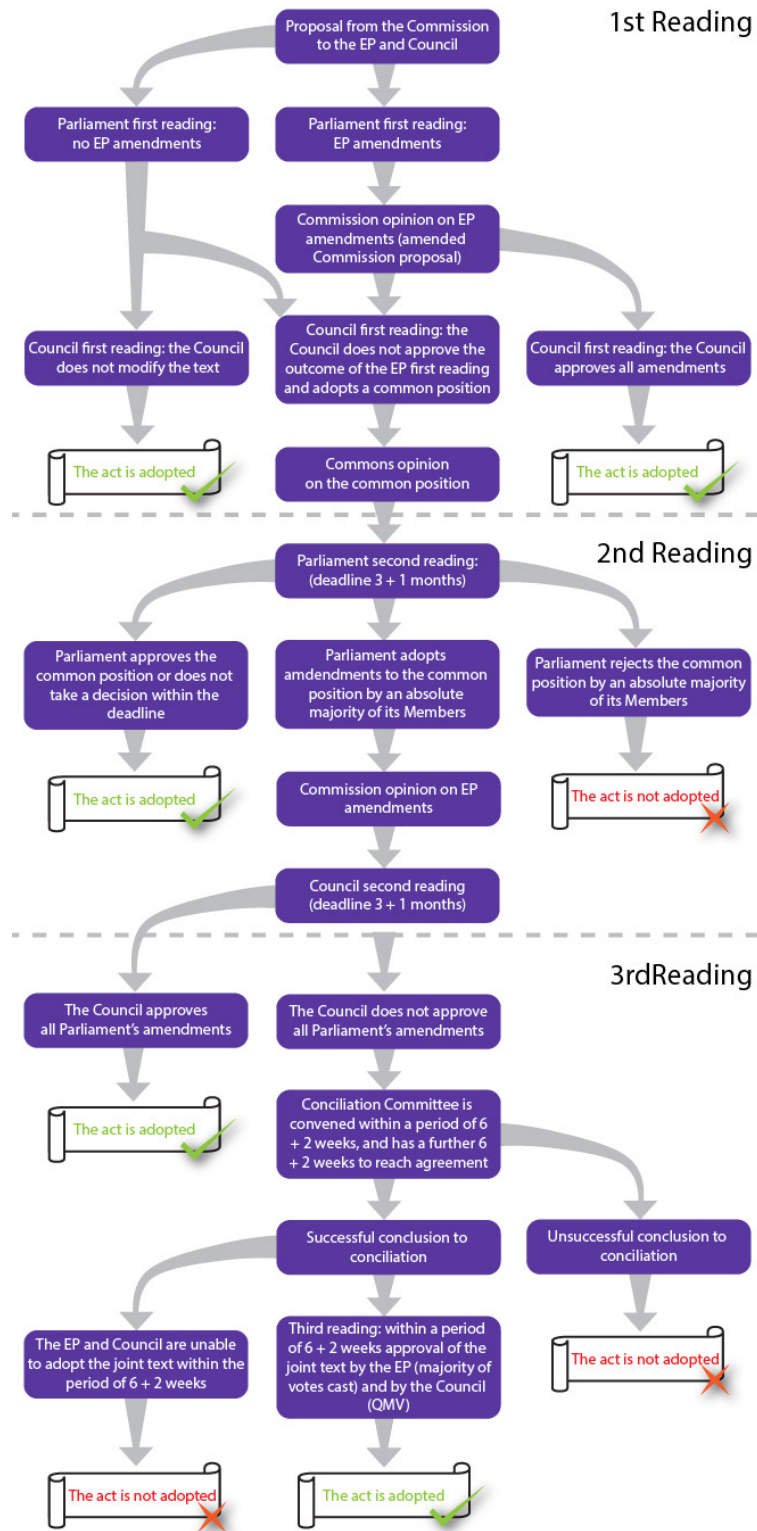


Figure B.3: Flowchart of how legislation passes through the EU [6]

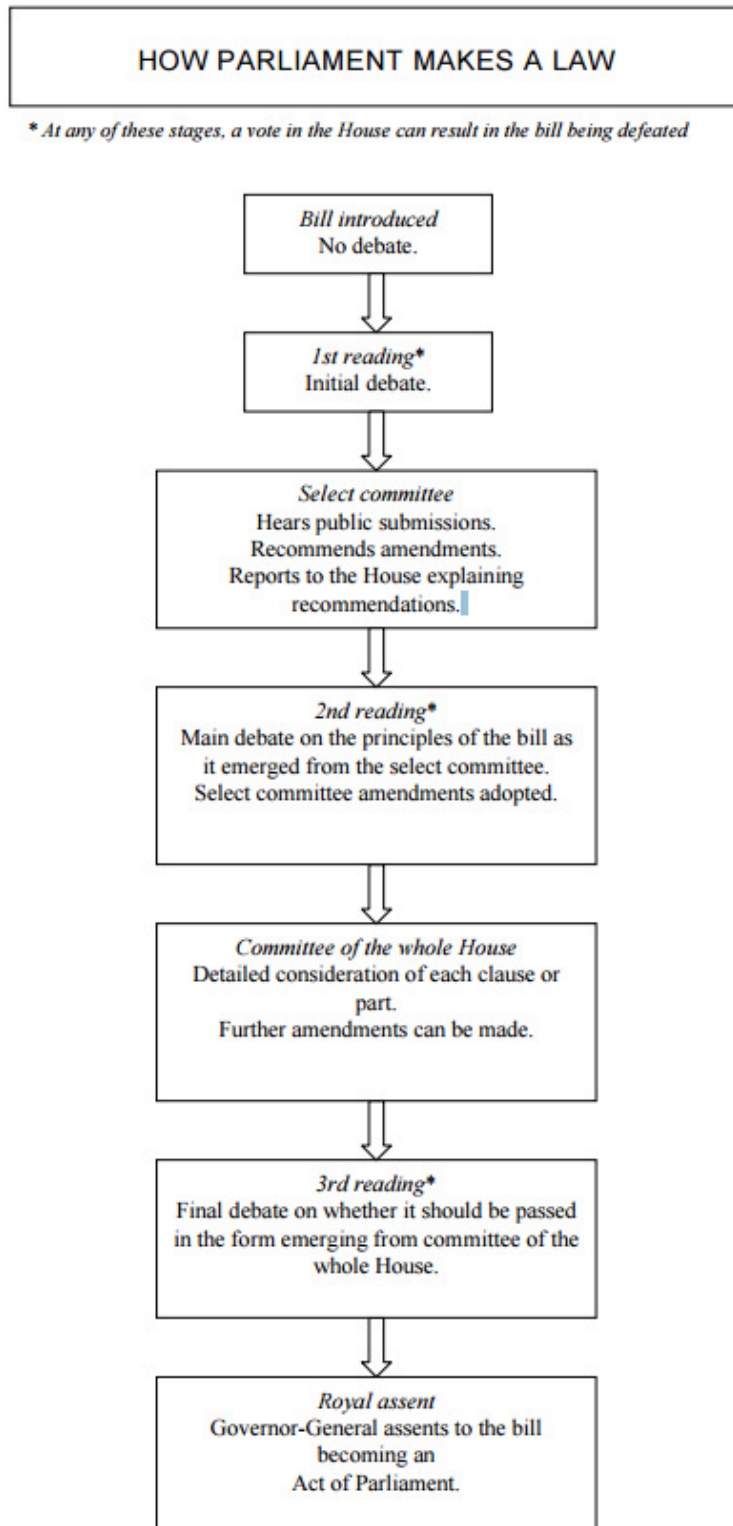


Figure B.4: Flowchart of New Zealand's legislative process [7]

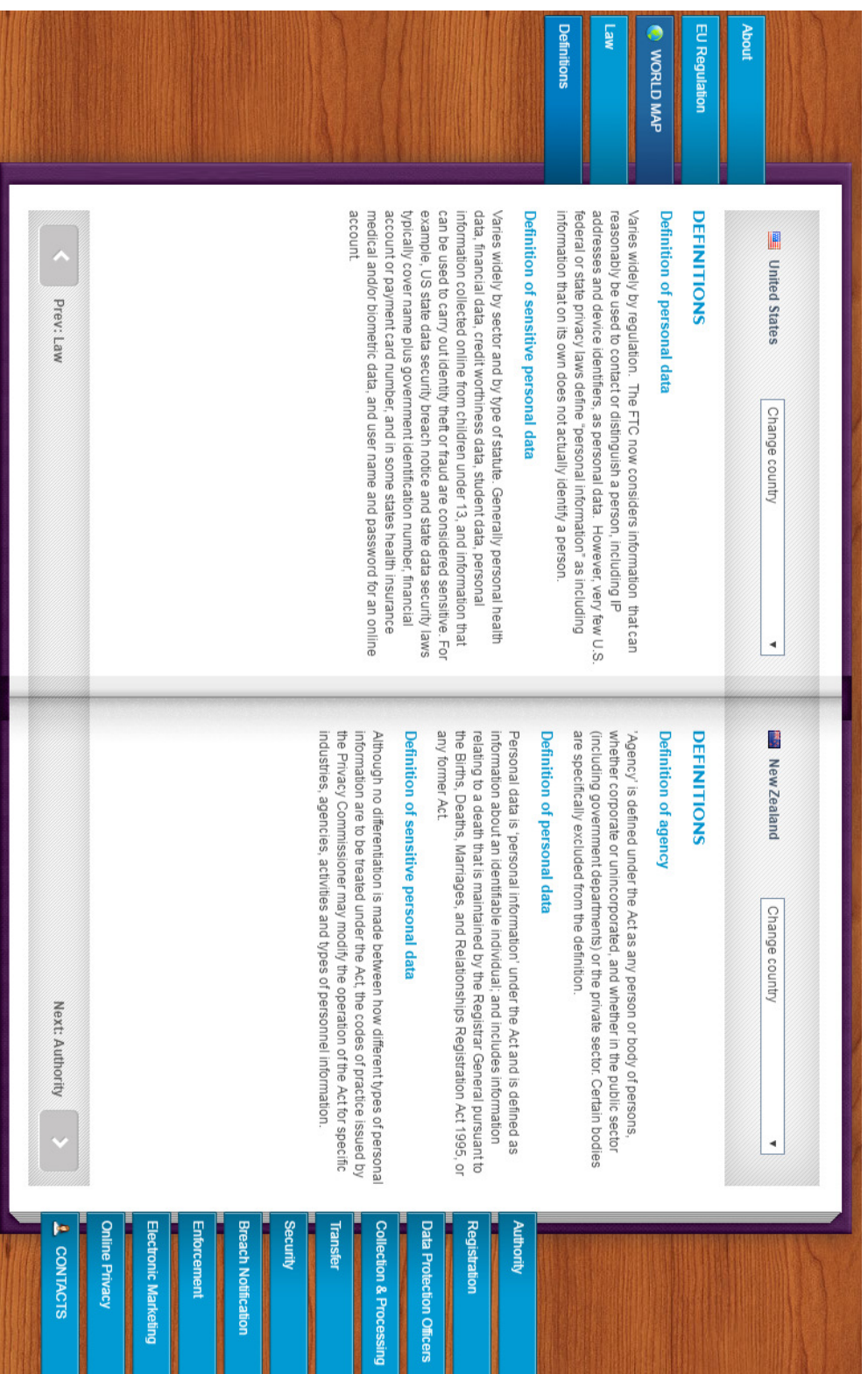


Figure B.5: Example of DLA Piper's Data Protection Laws of the World Handbook [8] which shows NZ compared with the US

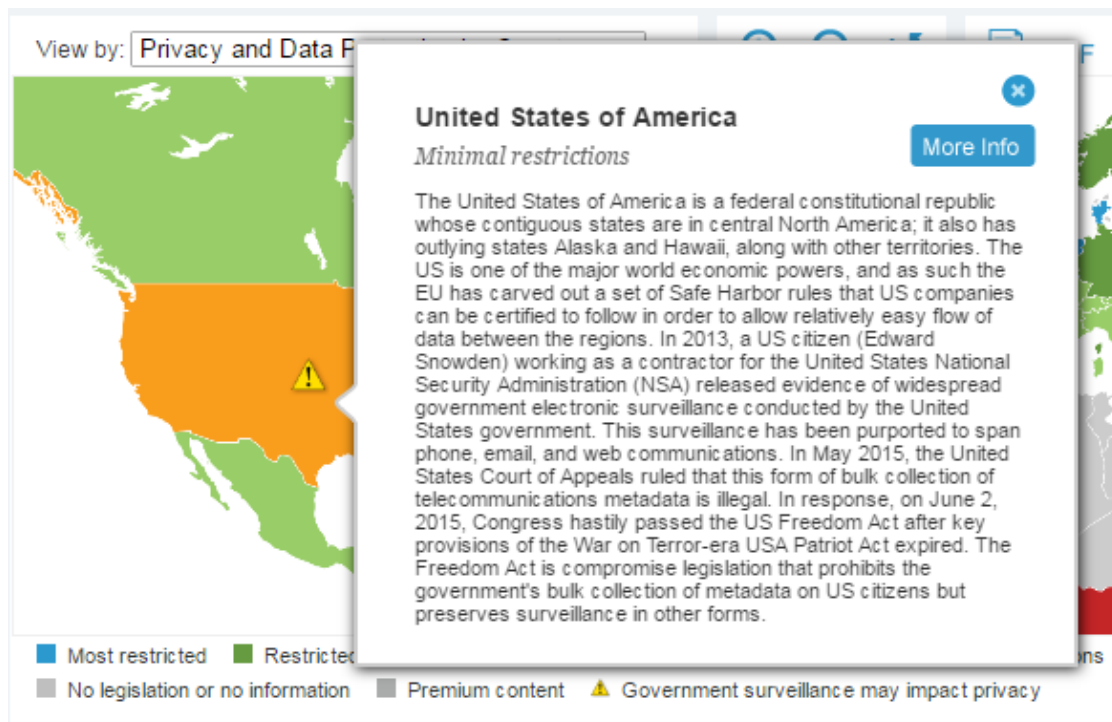


Figure B.6: Example of information for US from Forrester Global Heat Map

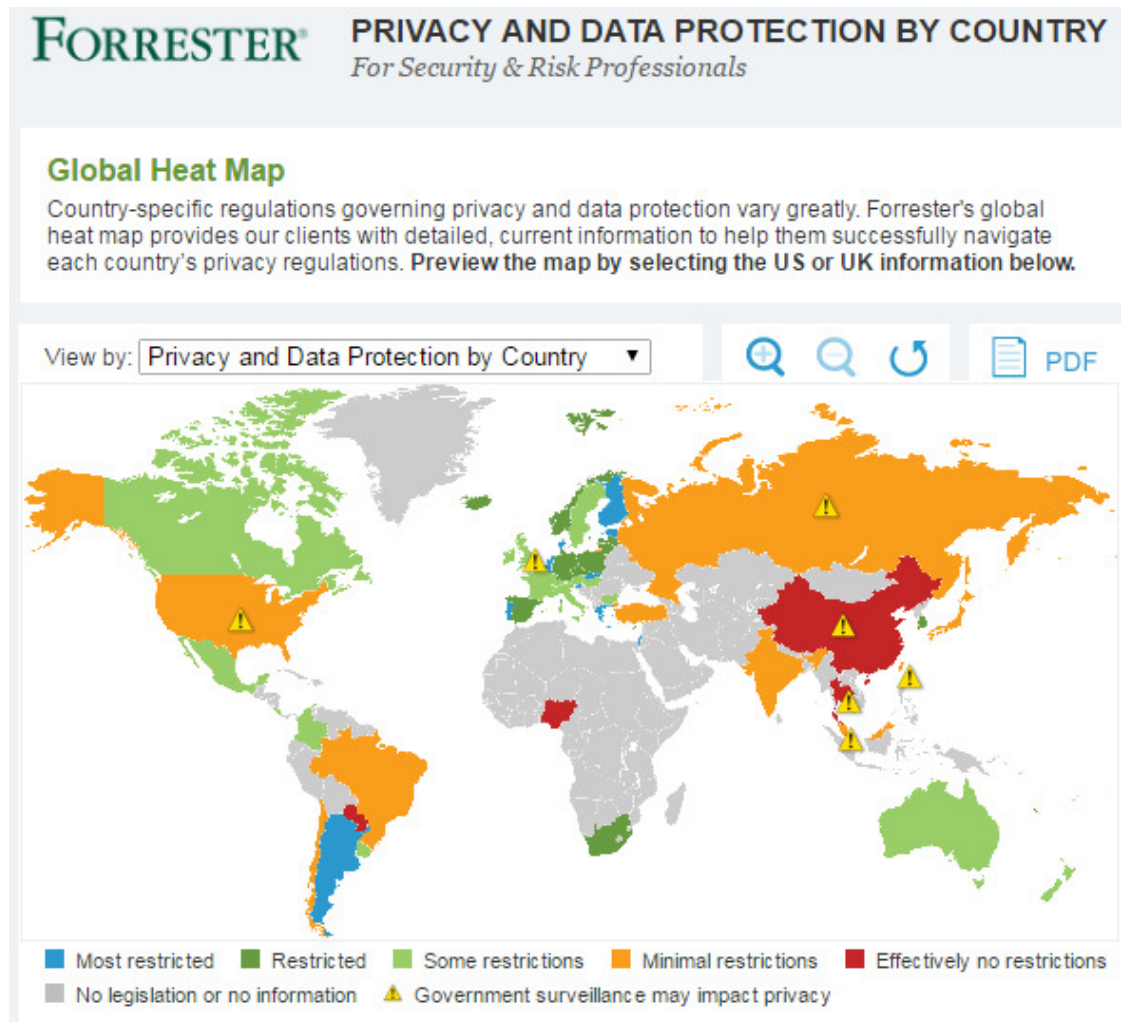


Figure B.7: Example screen shot of the Forrester Global Heat Map [9]

COUNTRY	LAW(s)/BILL(s)	STATUS	KEY DETAILS
Argentina	<i>Law for the Protection of Personal Data</i> (English language version: http://www.privacyinternational.org/countries/argentina/argentine-dpa.html)	Law enacted in November of 2000. Regulations for law enacted in December 2001.	Ensures notice, purpose limitation, data quality and security. Requires express consent for sensitive information. Data subjects have right to access, correct, block, or update data. Law enforced by national data protection commissioner (http://www.jus.gov.ar/minjus/DPDP/). Complaints may be brought before judicial system. Provides “adequacy” standards for data flows outside of Argentina. The European Union has determined that Argentina’s law meets the EU’s “adequacy” standard.

Figure B.8: Example of Argentina from the International Data Protection Legislation Matrix [10] produced by the US Department of Commerce

The screenshot displays a web application interface for the Baker & McKenzie's Global Privacy Handbook. The interface has a green header bar with navigation options: 'LAW APPLICABLE' (with a left arrow) and 'KEY PRIVACY CONCEPTS' (with a right arrow). Below the header, a dropdown menu is set to 'Australia'. The main content area is titled 'AUSTRALIA' and 'Personal Data'. It contains a definition of 'Personal information' from the Privacy Act, a bulleted list of criteria for identifying personal information, and a paragraph explaining the APP Guidelines. A red button labeled 'Compare Jurisdictions and Topics' is located on the right side of the content area. A close button (X) is in the top right corner of the header.

LAW APPLICABLE
Law Applicable

KEY PRIVACY CONCEPTS
Data Processing

Australia

AUSTRALIA
Personal Data

"Personal information" is defined in the Privacy Act as "information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not."

The APP Guidelines provide that the concept of information being "reasonably identifiable" can include information which is not "personal information" in its own right, can still come under the Privacy Act if there is a likelihood of it being combined with other information held by an organisation which would enable an individual to be reasonably identifiable.

Compare Jurisdictions and Topics

Figure B.9: Example summary from the Baker & McKenzie's Global Privacy Handbook

Adjust Current
Comparison



Adjust Current Comparison		»	
 Data Processing	Australia	Australia	Australia
	The APP's in the Privacy Act apply to the acts and practices of entities in respect of personal information, including in relation...	China	China
	United Kingdom	United Kingdom	United Kingdom
 Data Protection Officers	Australia	Australia	Australia
	In Australia, there is no requirement to appoint or designate a data privacy officer or other individual who will be accountable for the...	China	China
	United Kingdom	United Kingdom	United Kingdom

Figure B.10: Example of the Baker & McKenzie's Global Privacy Handbook showing the comparison of three countries and two topics [11]

Appendix C

Methodology Chapter Figures

ELEMENT PRESENT		New Zealand		China		Singapore
LEGISLATIVE FRAMEWORK	Has specific legislation enacted for data privacy	✓ Privacy Act 1993		✓ Telecommunications and Internet Personal User Data Protection Regulations 2013	✓ Personal Data Protection Act 2012	
	Has other legislation which covers data privacy	✓ Unsolicited Electronic Messages Act 2007		✓ Constitution of the People's Republic of China	✓ Spam Control Act 2008	
	Has civil and tortious liabilities for data privacy	×		✓ General Principles of Civil Law ✓ Tort Law of the People's Republic of China 2010 (Article 36)	×	
	Legislation in Government process	×		✓ Personal Data Protection Law	×	
	Implements Regulations	✓ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ✓ Health (Retention of Health Information) Regulations 1996		✓ The Decision of the Standing Committee of the National People's Congress on Strengthening the Network Information Protection 2012 (SIPoN) ✓ General Data Protection Law 2013 ✓ Law of the People's Republic of China on Protection of Consumer Rights and Interests 1994 ✓ Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems 2013 (PIP)	×	
DEFINITIONS						
PRIVACY AUTHORITY	"personal information" is defined	✓ Privacy Act 1993 section 2		✓ Telecommunications and Internet Personal User Data Protection Regulations 2013 Article 2	✓ Personal Data Protection Act 2012 section 2	
	"sensitive information" is defined	×		✓ PIP section 3.2	×	
	"Common Personal Information" is defined	×		✓ PIP section 3.7	×	
	"Explicit consent" is defined	×		✓ PIP section 3.8	×	
	"Tied consent" is defined	×		✓ PIP section 3.10	×	
COLLECTION AND USE OF INFORMATION	Has a protection authority	✓ Privacy Act 1993 section 12- Privacy Commission		×	✓ Personal Data Protection Act 2012 section 5 - Personal	
	Functions of authority are clearly set out	✓ Privacy Act 1993 section 13		NA	✓ Personal Data Protection Act 2012 section 6	
	Agencies Required to appoint privacy officer	✓ Privacy Act 1993 section 23		×	✓ Personal Data Protection Act 2012 section 11 (3)	
	Agencies Required to register	×		×	×	
	Privacy Officers details made available	×		×	×	
Purpose needs to be explained	Have in place policies and practices for personal information	✓ But Privacy Commissioner may make a request		×	✓ Personal Data Protection Act 2012 section 11 (5)	
		×		✓ Internet Personal User Data Protection Regulations Article 8	✓ Personal Data Protection Act 2012 section 12	
		✓ Privacy Act 1993 section 6 principle 3		✓ PIP section 5.1	✓ Personal Data Protection Act 2012 section 12	
		✓ OECD Guidelines for Privacy, Part II, 9		✓ SIPoN article 2	✓ Personal Data Protection Act 2012 section 18-20	
		✓ Privacy Act 1993 section 6 principle 3		✓ Consumer Rights and Interests article 29 ✓ Internet Personal User Data Protection Regulations Article 9 ✓ PIP section 4.2 a ✓ SIPoN article 2	✓ Personal Data Protection Act 2012 section 18-20	

Figure C.11: Example First Draft of the Waikato Data Privacy Matrix

PRIVACY MATRIX VERSION 0.2		APAC Countries									
Control Domain	Domain Code	Control Specification	New Zealand			Australia			China		
			Document name	Notes	Document name	Notes	Document name	Notes	Document name	Notes	Single
Legislative Framework	LEG-04	Local government has no Bill going through the legislative process			Privacy Amendment (Disclosure of Serious Data Breaches) Bill 2015		Personal Data Protection Law of the People's Republic of China				
Legislative Framework	LEG-05	Regulations, standards or guidelines that are issued and followed that have relation to data privacy	Health (Retention of Health Information) Regulations 1998		Australian Privacy Principles guidelines (part of Privacy Act 1988)		Personal Information Protection Law of the People's Republic of China (2017) (PIPL)				
Legislative Framework	LEG-06	Clf or robust liabilities available for data privacy			Convention on Cybercrime		General Principles of Civil Law of the People's Republic of China 2010 (outside 38)				
Privacy Body	PRV-01	There is a requirement to establish a privacy authority to oversee privacy issues			Privacy Act 1988 Section 62	The establishes the Privacy Advers Committee			Personal Data Protection Act 2012 Section 5		Establishes it
Privacy Body	PRV-02	There is a requirement to establish a privacy commissioner		This establishes the Privacy Commissioner	Privacy Act 1988 Section 27	Establishes 3 roles: Privacy Commissioner, the Privacy Commissioner and the Freedom of Information Commissioner					
Privacy Body	PRV-03	The functions of the authority clearly set out			Privacy Act 1988 Section 14		Privacy Act 1988 Section 83		Personal Data Protection Act 2012 Section 6		
Privacy Body	PRV-04	There is a requirement each company establishes their own privacy officer to ensure the company complies with policy			Privacy Act 1988 Section 23	Not required but is recommended by the Information Commissioner		This is not a requirement but is recommended that a "Data Controller" is appointed	Personal Data Protection Act 2012 Section 11(3)		Data Protect
Privacy Body	PRV-05	Contract details of the privacy officer are made available		At least one officer needs to be elected					Personal Data Protection Act 2012 Section 11(3)		
Privacy Body	PRV-06	Each company to have an internal privacy policy proposed and approved			Privacy Act 1988 Schedule 1 Principle 1				Personal Data Protection Act 2012 Section 12		
Privacy Body	PRV-07	An internal audit process is outlined for each company		Section 13 of the Privacy Act gives the commissioner the power to audit if required		Section 13 of the Privacy Act gives the commissioner the power to audit if required			Personal Data Protection Act 2012 Section 12		The Privacy Act 2012 provides for audit current
Pre Collection Process	PCP-01	"Personal information" is defined which gives examples and a clear outline	Privacy Act 1988 Section 2		Privacy Act 1988 Section 6	Telecommunications (Interception and Access) Act 1979 (TIAA) (Part 1.1b)	OECD Guidelines for Privacy (Part 1.1b)	APAC Privacy Guidelines Principle 3	Personal Data Protection Act 2012 Section 12		Personal Data Protection Act 2012 Section 12

Figure C.13: Example of the Waikato Data Privacy Matrix final version

Appendix D

Verification From Experts

D.6 Katrine Evans [1]

LEG-02

I was trying to think what else might be relevant to cloud. Worth mentioning the GCSB and SIS legislation probably, as they can get access under security warrant. The Telecommunications Act itself is worth a mention too. TICS is more about interception capability.

In the notes column, mention section 7 of the Privacy Act - it states that if other legislation is inconsistent with the Privacy Act, the other legislative provision will override the Privacy Act's principles.

LEG-03

The things listed aren't regulations, of course - they have no formal legal effect in New Zealand. They relate to organisations that we participate in, for sure, but the reference to regulations is a bit misleading. I'd at least clarify in the notes that they have no formal legal effect (you can't sue under them, for instance).

Since they're not directly applicable in NZ (at best they're interpretation tools), you might want to tweak whether or how you refer to them later? I'd probably delete them from those later parts of the matrix altogether.

LEG-04

May be worth adding note that the privacy reforms are still in the policy process - no draft legislation has been introduced yet.

LEG-05

It's worth adding a reference to DIA's guidance on cloud computing:

<https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing/>.

The Privacy Commissioner's guidelines are at

<https://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-Cloud-Computing-guidance-February-2013.pdf>

There's also the Cloud Code: <https://cloudcode.nz/>

These are all in the guidance area rather than having more formal force, but are useful.

PRI-01

This overlaps with PRI-02 of course - the privacy commissioner is a privacy authority.

PRI-02

Given the overlap with PRI-01, I wonder if it would be more useful to focus on whether the privacy authority is independent of government or other external control (the answer to which in NZ of course is yes).

PRI-03

There are a few functions that aren't listed in section 13, eg complaint investigation (part 8), supervision of information matching agreements (part 10) and consultation, reporting and review of approved information sharing agreements (part 9A). But I don't know how granular you want to get.

PRI-05

Worth a note saying that this is expected practice?

PRI-06

Principle 3 deals with some of this.

PRI-07

The audit function in s13 isn't a power to audit - the Commissioner can only audit on request from the agency under that provision. So this needs adjusting

PCP-01

This is where the references to the OECD and APEC docs start, and I think it's best to delete them from the NZ column. May well be worth while having a separate column for each.

PCP-02

Note: there is no formal distinction in NZ between personal information and sensitive personal information. However, sensitivity of the information is a factor that can affect legal obligations in certain circumstances, particularly when deciding whether collection is "necessary" (principle 1) or whether security standards are reasonable in the circumstances (principle 5)

PCP-03

Principles 2 and 10 also refer to publicly available information. Part 7 deals with public register information - there is a set of 4 public register privacy principles. Not all organisations are covered by the Privacy Act though most are - is this worth mentioning? The definition of "agency" excludes some bodies, including courts in relation to judicial functions.

PCP-04

Principle 3 isn't a consent provision. It's a transparency provision - still very useful, but falls short of requiring consent.

Authorisation (express or implied) is an exception to a few of the principles though (2,10 and 11). The agency is allowed to collect from third parties, or use and disclose for different purposes if this is authorised by the individual concerned.

PCP-06

For most transactions, consent can either be written or verbal. (Written is clearer, of course, but not legally required in most circumstances).

PCP-07

The Privacy Act itself doesn't differentiate based on age. In practice, however, the parent or guardian of a child who's too young to express their own views will be treated as the representative of that child.

PCP-08

Principle 9 doesn't usually imply that one can withdraw consent (though it would be nice if it did!). It's more geared to the agency's own purposes for keeping information.

PCP-09

It's principle 3 that says the purpose has to be explained to the individual. Principle 1 requires the agency to have a lawful purpose though - and the collection has to be necessary for that purpose too.

PRO-03

May be worth noting that the principal agency remains liable even if information is in the hands of a third party data processor. Section 10 also allows information to be sent offshore.

PRO-04, PRO-07

There are exceptions to principles 10 and 11 - eg maintenance of law, safety, court proceedings. So there are some limitations on the proposition in the question.

PRO-0

This is usually a principle 5 issue. The government agency reference relates to information matching programmes rather than more widely.

PRO-06

Worth noting the limitations on assigning unique IDs?

PRO-08, STO-08

The offences in s127 don't help here - they're not relevant. There's a civil enforcement regime, though, through the Human Rights Review Tribunal which can make orders and award compensation for harm.

STO-03, 04

Again section 10 might be relevant. Under principle 3 people also have to be told.

STO-05

A principle 5 issue, probably (all the storage stuff is). Not sure what the note means - a reference to keeping some kinds of highly sensitive/confidential information onshore to prevent access by foreign governments/foreign court orders? Section 10 says if info subject to foreign law, it won't be a breach to release it...

STO-07

Existence of policies not in the leg' but it's hard to show you comply with principle 5, or principle 9 for instance if you don't have them ...

STO-09

We don't have mandatory breach notification in NZ. So the answer is no. The note can say that it's considered best practice, and refer to the data safety toolkit.

STO-10

Possibly a principle 5 issue, but it's a problem that the legislation doesn't fully address. Eg no rules on data portability

SPM-05

May be worth note that Marketing Association scheme is self-regulatory. Unlike the Australian equivalent I don't think it covers mobile numbers (it certainly used not to cover mobile)

INT-01

Agencies aren't always required to notify the individual. There are some legal

barriers to providing information about the existence or content of interception warrants eg Telecommunications Act.

INT-03

I haven't checked the provisions, sorry, but under the Search and Surveillance Act I don't think warrants are always required (they may always be required for interception as such though - worth checking)

INT-05

Note may be a little provocative. There are certainly information sharing arrangements in place with external agencies - that's less speculative.

D.7 Neil Sanson [2]

LEG-02 Other legislation

This could be very broad and might include, for example:

Tax Administration Act

Birth Deaths Marriages and Relationship Registration Act

Public Records Act

Statistics Act

Coroners Act

LEG-05 regulations

I would suggest including the Protective Security Requirements (which include the NZISM)

You might also want to include codes under the Privacy Act.

PRO-07

I suggest also Principle 5(a)(ii).

STO-03

I am not sure why Principles 3 and 10 are referenced. Principle 11 seems more directly appropriate.

STO-04

I am not sure why Principles 3 and 10 are referenced. Principle 5 and Section 10 seem more directly appropriate.

STO-05

I am not sure why Principles 3 and 10 are referenced.

STO-06

I suggest adding Principle 5.

STO-07

I suggest adding Principle 9 and Principle 5.

STO-08

I suggest the Note could be the same as for PRO-08.

I have attached two unpublished documents that may be of interest. They are not necessarily up to date or complete. The Legislative Responsibilities document was last updated in 2015. The Information Sharing Provisions document was updated in 2016 but only limited searching for new legislative provisions was conducted because of the difficulty of identifying the necessary search terms.

D.8 Michael Dizon [3]

LEG-01

- data privacy is connected to but is not the same as data protection; data privacy

is the broader concept that includes data protection; most of the laws cited are data protection laws

- it might be good to distinguish between "privacy", "data privacy" and "data protection" in the definitions section

LEG-03

- I wouldn't say that the EU Data Protection Directive a mere "guideline"; you could call it a legal framework or regime

PR-01 and PR-02

- privacy and data protection are related concepts but are not the exactly the same; privacy is the broader concept; even a privacy commissioner is mostly concerned with data protection
- it might be better to use the term "data protection authority" since this indicates what they actually do

STO-10 and 11

- what is a data collection agency? are you referring to a "data broker"?

INT-01 and 02

- why use data collection agency? you might want to use "data controller" and/or "data processor" instead

INT in general

- there are other procedural measures that are provided for under the Convention on Cybercrime and corresponding national cybercrime laws that have an impact on data protection
- these procedural measures include: (a) expedited preservation of stored computer data; (b) expedited preservation and partial disclosure of traffic data; (c) production orders; (d) search and seizure of stored computer data; (e) real-time collection of

traffic data; (f) interception of content data; and (g) destruction of computer data

D.9 Alan Shipman [4]

UK section

With the UK's 'Brexit' referendum results, the UK will no longer be a member of the EU in due course. This will not be before the EU's GDPR comes into effect on 25th May 2018. The UK's supervisory authority (The Information Commissioner) has stated that the GDPR will be implemented within the UK and is currently working on legislation to deal with this issue. The legislative framework in the UK will change over the next couple of years.

The EU-US agreement has been superseded by the Privacy Shield process (the Safe Harbour process has been withdrawn) *[http : //ec.europa.eu/justice/data – protection/files/factsheets/factsheet_eu – us_privacy_shield_en.pdf](http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf)* However, there are still debates about the adequacy of this process so changes may occur in due course.

PRI-04 to 07 notes need to be updated – the GDPR requires a designated data protection officer under some circumstances (GDPR Recital 97, Article 37). There is no such requirement under current legislation.

PCP, PRO, STO, SPM, INT – a lot of this will change over the next couple of years, taking into account the GDPR

Appendix E

Additional Results Chapter

Figures

Figure E.14: A screen shot of the Australian Privacy Act 1988 online version [12



Privacy Act 1993

Public Act 1993 No 28
 Date of assent 17 May 1993
 Commencement see section 1(2)

Note

Changes authorised by [subpart 2](#) of Part 2 of the Legislation Act 2012 have been made in this official reprint.

Note 4 at the end of this reprint provides a list of the amendments incorporated.

This Act is administered by the Ministry of Justice.

Contents

	Title
1	Short Title and commencement
	Part 1
	Preliminary provisions
2	Interpretation
3	Information held by agency
4	Actions of, and disclosure of information to, staff of agency, etc
5	Act to bind the Crown
	Part 2
	Information privacy principles
6	Information privacy principles
7	Savings
8	Application of information privacy principles
9	Postponement of application of principle 11 to lists used for direct marketing
10	Application of principles to information held overseas
11	Enforceability of principles
	Part 3
	Privacy Commissioner
12	Privacy Commissioner
13	Functions of Commissioner

Figure E.15: A screen shot of the New Zealand Privacy Act 1993 online version

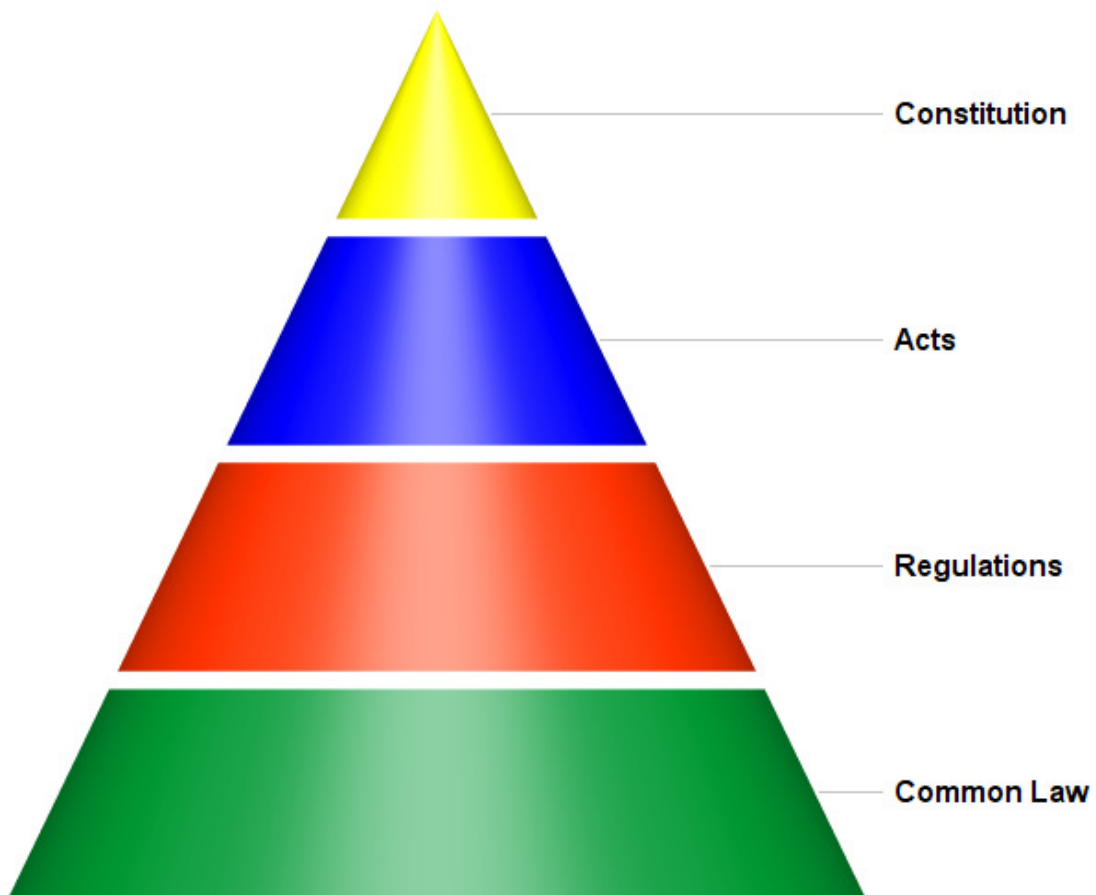


Figure E.16: Example of a Generic Legislative Hierarchy which applies to the EU and APAC regions

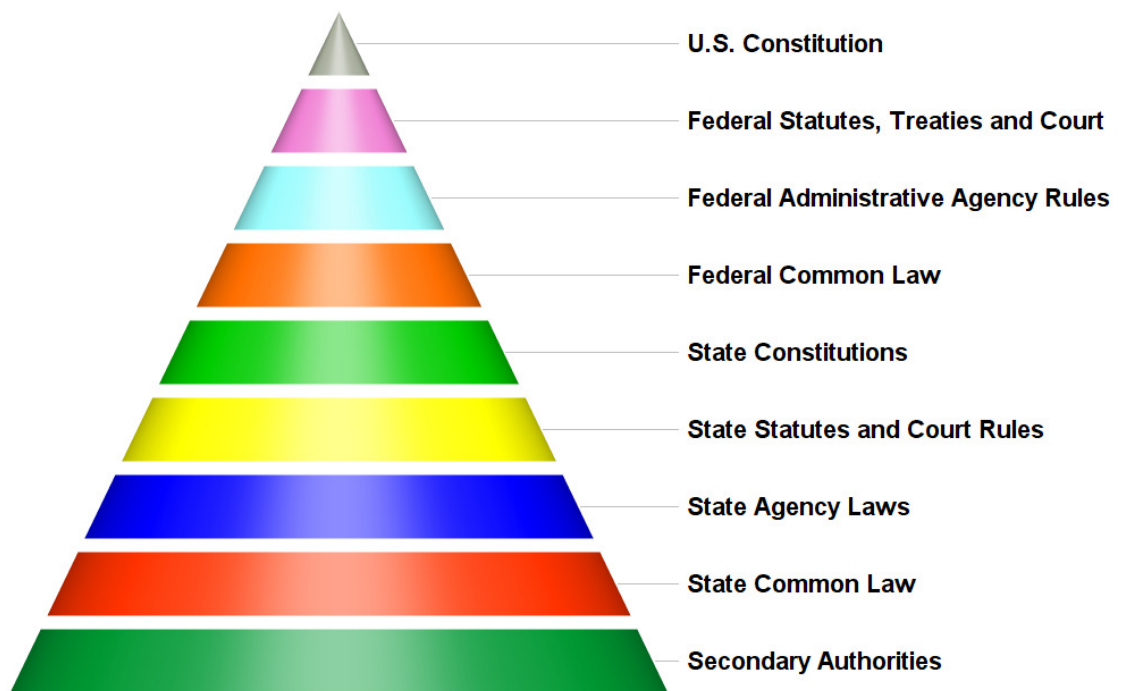


Figure E.17: Example of the United States Legislative Hierarchy

Appendix F

Conclusion Figures

<div><div><div><div></div><div>Waikato Data Privacy Matrix</div><div>Version 0.6</div></div></div></div>														
			Asia Pacific Countries								European Union Countries			
Control Domain	Domain Code	Control Specification	New Zealand		Australia		China		Singapore		Malaysia		United Kingdom	
			Document name	Notes	Document name	Notes	Document name	Notes	Document name	Notes	Document name	Notes	Document name	Notes
Legislative Framework	LEG-01	Legislation enacted specifically for data privacy?	<ul style="list-style-type: none">Privacy Act 1993		<ul style="list-style-type: none">Privacy Act 1988Australian Information Commissioner Act 2010		<ul style="list-style-type: none">Telecommunications and Internet Personal User Data Protection Regulations 2013 (TIPIP)General Data Protection Law 2013		<ul style="list-style-type: none">Personal Data Protection Act 2012		<ul style="list-style-type: none">Personal Data Protection Act 2010		<ul style="list-style-type: none">Data Protection Act 1998	
Legislative Framework	LEG-04	Local government has any Bills going through the legislative process	<ul style="list-style-type: none">Privacy Act 1993 Reform	Draft legislation is yet to be introduced.	<ul style="list-style-type: none">Privacy Amendment (Notification of Serious Data Breaches) Bill 2015		<ul style="list-style-type: none">Personal Data Protection LawCybersecurity Law of the People's Republic of China						<ul style="list-style-type: none">General Data Protection Regulation	This will be a replacement for the current DPD (From 25 May 2018)
Legislative Framework	LEG-05	Regulations, standards or guidelines that are implemented and followed that have relation to data privacy	<ul style="list-style-type: none">Requirements for Cloud Computing (RCC)Cloud Computing Guidelines (CCG)New Zealand Cloud Code NZSOM Part 1NZSOM Part 2Telecommunications Information Privacy Code 2003Codes of Practice under Part VI of the Privacy Act	RCC is from the New Zealand Department of Internal Affairs CCC is from the office of the Privacy Commissioner. Cloud Code is from Institute of IT Professionals New Zealand.	<ul style="list-style-type: none">Australian Privacy Principles Guidelines (part of Privacy Act 1988)Convention on Cybercrime 2001		<ul style="list-style-type: none">Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems 2013 (IPIS)						<ul style="list-style-type: none">Telecommunications (Data Protection and Privacy) Regulations 1999Convention on Cybercrime 2001	
Legislative Framework	LEG-06	Has other state laws related to privacy. Note these will not be identified as too extensive												
Privacy Body	PRI-01	There is a requirement to establish a privacy authority to oversee privacy issues			<ul style="list-style-type: none">Privacy Act 1988 Section 82	This establishes the Privacy Advisor Committee			<ul style="list-style-type: none">Personal Data Protection Act 2012 Section 5	Establishes the Personal Data Protection Commission	<ul style="list-style-type: none">Personal Data Protection Act 2010 Section 70	establishes the Personal Data Protection Advisory Committee	<ul style="list-style-type: none">Communications Act 2003 Section 1	The Communications Act sets up The Office of Communications (OFCOM). The Information Commissioner's Office (ICO) is an independent authority
Privacy Body	PRI-07	An internal audit process is outlined for each company				Section 33 C of the Privacy Act gives the commissioner the power to audit if required				The Personal Data Protection Commission recommends the Data Protection Officers utilize their "Personal Data Protection Checklist for Organisations". This will help to audit current policies.	<ul style="list-style-type: none">Personal Data Protection Act 2010 Section 101	Personal Data Protection Commissioner may carry out an inspection of any personal data systems.		
Pre Collection Process	PCP-01	"Personal Information" is defined which gives examples and a clear outline	<ul style="list-style-type: none">Privacy Act 1993 Section 2OECD Guidelines for Privacy, Part I, 1 (b)		<ul style="list-style-type: none">Privacy Act 1988 Section 6Telecommunications (Interception and Access) Act Section 187LA		<ul style="list-style-type: none">TIPIP Article 8PIP Section 3.2		<ul style="list-style-type: none">Personal Data Protection Act 2012 Section 2	Personal Data	<ul style="list-style-type: none">Personal Data Protection Act 2010 Section 4	Personal Data	<ul style="list-style-type: none">Data Protection Act 1998 Section 1CIB Article 2 (a)	Personal Data
Pre Collection Process	PCP-07	Level of consent different for different age groups				There is no specific age for consent but the Australian Privacy Principles Guidelines give some guidance in Sections 8.50 - 8.52. As long as the individual has "sufficient understanding and maturity to					<ul style="list-style-type: none">Personal Data Protection Act 2010 Section 4	"relevant person" - (a) in the case of a data subject who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the data subject;		
Pre Collection Process	PCP-08	Consent may be withdrawn at any time			<ul style="list-style-type: none">Australian Privacy Principles guidelines 8.45		<ul style="list-style-type: none">PIP Section 5.5.1SNIP Article 8TIPIP Article 9		<ul style="list-style-type: none">Personal Data Protection Act 2012 Section 16		<ul style="list-style-type: none">Personal Data Protection Act 2010 Section 38		<ul style="list-style-type: none">Data Protection Act 1998 Section 10	
Data Processing	PRO-01	Individual has the ability to access their data by request	<ul style="list-style-type: none">Privacy Act 1993 Section 6 Principle 6		<ul style="list-style-type: none">Privacy Act 1988 Schedule 1, Principle 12		<ul style="list-style-type: none">TIPIP Article 9PIP Section 5.3.7		<ul style="list-style-type: none">Personal Data Protection Act 2012 Section 21		<ul style="list-style-type: none">Personal Data Protection Act 2010 Section 12 and 30		<ul style="list-style-type: none">Data Protection Act 1998 Section 7Freedom of Information Act 2000 Section 8CIB Article 13	
Data Processing	PRO-09	A complaints process is setup to deal with any breach of privacy	<ul style="list-style-type: none">Privacy Act 1993 Section 67		<ul style="list-style-type: none">Privacy Act 1988 Schedule 1, Principle 1		<ul style="list-style-type: none">SNIP Article 11TIPIP Article 12PIP Section 5.2.2.h		<ul style="list-style-type: none">Personal Data Protection Act 2012 Section 12 and 27 - 32		<ul style="list-style-type: none">Personal Data Protection Act 2010 Section 104		<ul style="list-style-type: none">Data Protection Act 1998 Section 42Communications Act 2003 Section 52 (2)	DPA refers to this as a Request for Assessment, Section 43 then outlines "Information Notices"
Data Storage	STO-09	Notification has to be given to individuals in case of a data breach		This is considered best practice suggested in the Data Safety Toolkit		Data breach policy and response plan recommended	<ul style="list-style-type: none">PIP Section 4.1.3	This is not a requirement but a suggested action taken by Personal information administrators						
Data Storage	STO-10	Policy in place in case data collection agency ceases to operate					<ul style="list-style-type: none">PIP Section 5.5.4							
Data Storage	STO-11	Policy in place in case data collection agency is sold												
Spam	SPM-01	A clear unsubscribe feature is available	<ul style="list-style-type: none">Unsolicited Electronic Messages Act 2007 Section 11		<ul style="list-style-type: none">Spam Act 2003 Section 18		<ul style="list-style-type: none">Regulations On Internet Email Services 2006 Article 14	Does not mention an "unsubscribe feature"	<ul style="list-style-type: none">Spam Control Act 2008 SECOND SCHEDULE Section 2					
Spam	SPM-02	Commercial electronic messages contain clear and accurate contact information about the sender	<ul style="list-style-type: none">Unsolicited Electronic Messages Act 2007 Section 10		<ul style="list-style-type: none">Spam Act 2003 Section 17		<ul style="list-style-type: none">Regulations On Internet Email Services 2006 Article 14		<ul style="list-style-type: none">Spam Control Act 2008 SECOND SCHEDULE Section 3(d)				<ul style="list-style-type: none">PEC Section 23	Section 24 relates to automated calling, facsimile and automated calling
Spam	SPM-07	Unsolicited commercial electronic messages are prohibited to other countries	<ul style="list-style-type: none">Unsolicited Electronic Messages Act 2007 Section 9	The definition in Section 4 of a "New Zealand Link" may be needed for further explanation	<ul style="list-style-type: none">Spam Act 2003 Section 16	The definition in Section 7 of a "Australian Link" may be needed for further explanation			<ul style="list-style-type: none">Personal Data Protection Act 2012 Section 11	The definition in Section 7 of a Singapore Link" may be needed for further explanation				
Interception of Data	INT-01	A data collection agency required to notify the individual if they have been requested to hand over persons information	<ul style="list-style-type: none">GCSB Section 15E											
Interception of Data	INT-05	External countries have the ability to intercept data with permission from the host country			<ul style="list-style-type: none">TIA Division 3						<ul style="list-style-type: none">Communications and Multimedia Act 1998 Section 269		<ul style="list-style-type: none">Regulation of Investigatory Powers Act 2000 Section 1 (4), 6 (2)(i)	

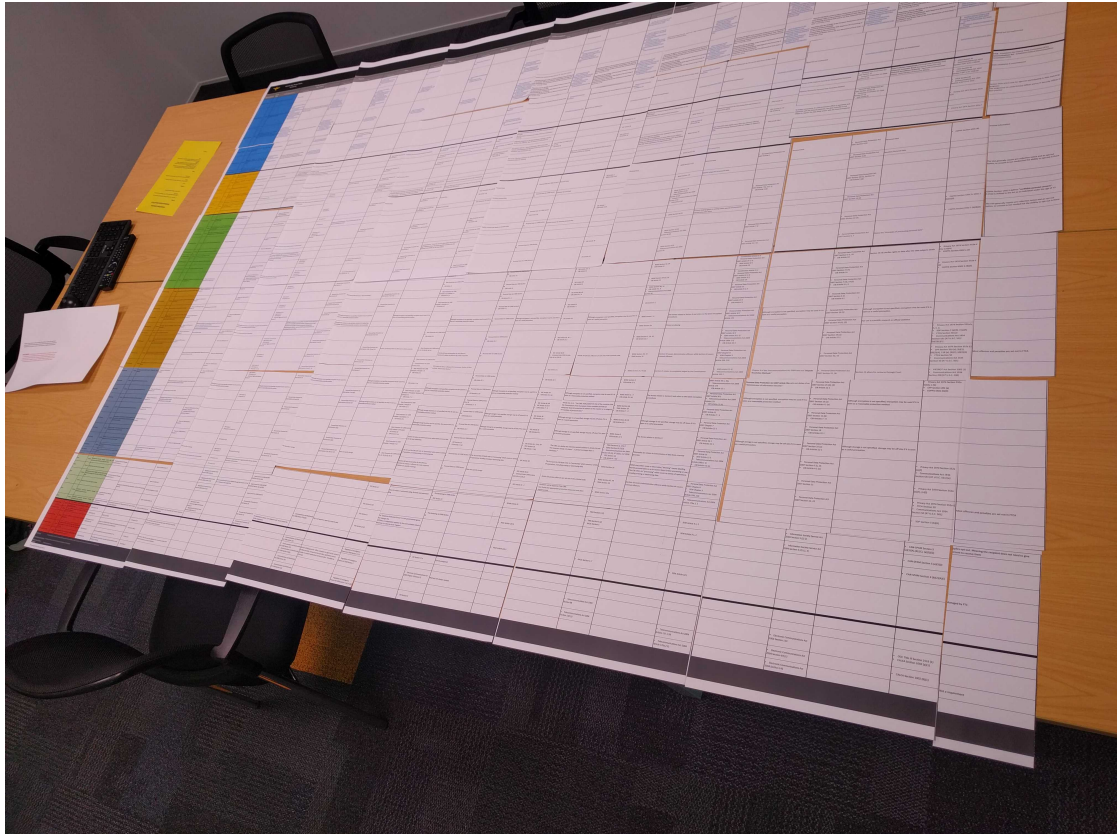


Figure F.18: This photo shows the size of the Waikato Data Privacy Matrix, which covers 42 A3 pages when printed

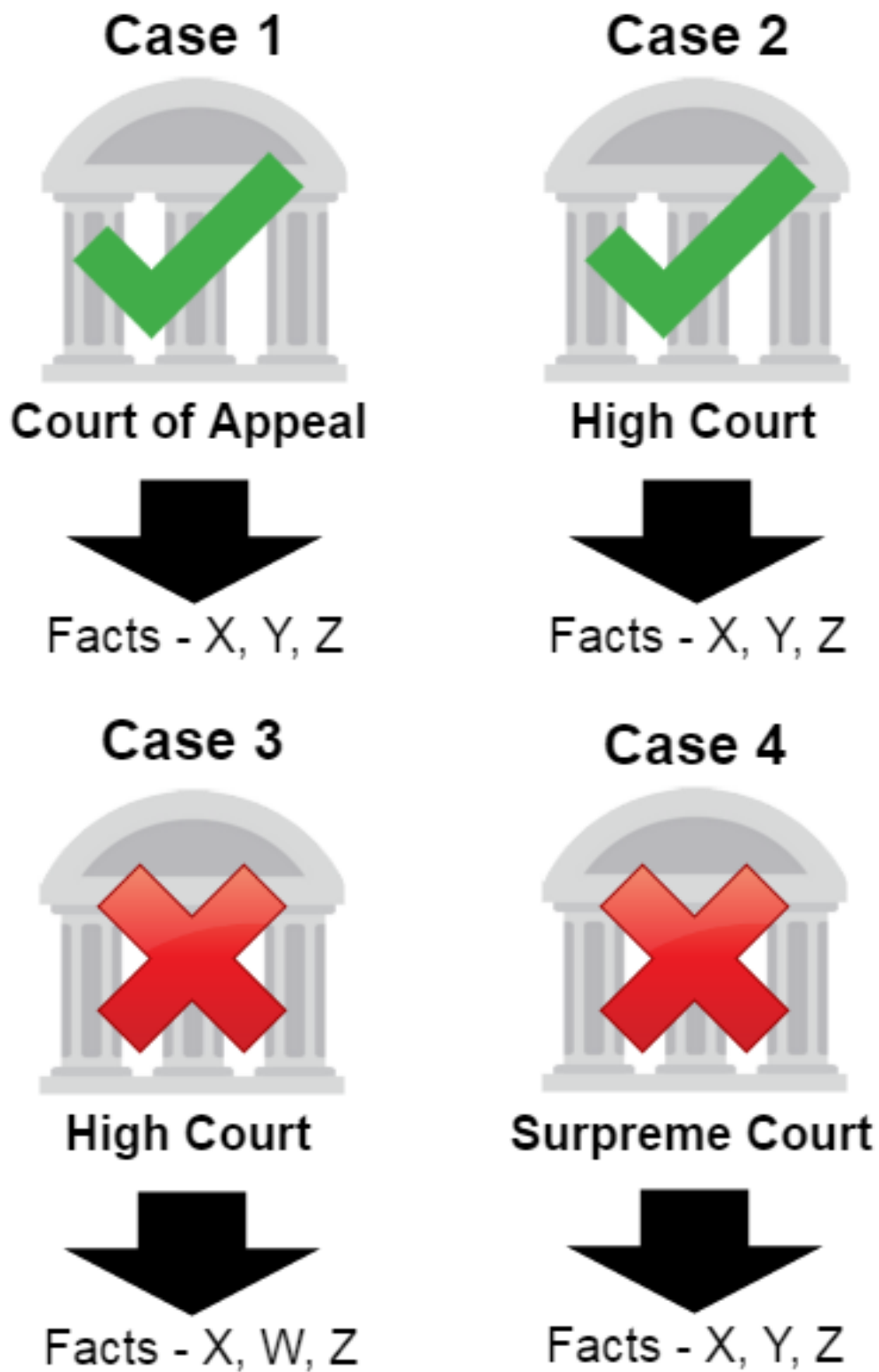


Figure F.19: Example of how case law binds lower courts providing facts of the case are the same or similar