The Data Privacy Matrix Project: Towards a Global Alignment of Data Privacy Laws

Craig Scoon
Cyber Security Lab
The University of Waikato
Hamilton, New Zealand
Email: craigscoon@gmail.com

Ryan K L Ko
Cyber Security Lab
The University of Waikato
Hamilton, New Zealand
Email: ryan@waikato.ac.nz

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

This paper will introduce our global project for data privacy by focusing on Asia Pacific data privacy laws and their relationships with the European Union and the USA. This will also suggest potential solutions to address some of the issues which may occur when a breach of data privacy occurs, in order to ensure an individual has their data privacy protected across the boundaries in the Web.

I. Introduction

Privacy has always been a contentious issue within the legal realm. The laws filter down through governments to society and by this point become very unclear. In recent years there has been much media coverage and publicity about leaks of personal data and breaches of data privacy, most of which came from the 2013 National Security Agency (NSA) leaks. The outcome of these leaks has again highlighted the need for clarification around trans-national legislation and a way of aligning legislation for the everyday user to understand

The fast paced evolution in the area of the Internet of Things (IoT) makes this domain a vital step that cannot be overlooked to ensure users can trust these technologies and services. The amount of data and personal information that is being stored or transferred to servers inside or outside of the legal jurisdiction that the device resides in, creates a need for users and vendors to have a better understanding of these global data privacy legislations that may create repercussions for their business or privacy.

One example of how the legislation differs from country to country is by looking at a simple term like "sensitive data". Throughout the Asia Pacific (APAC) countries China, Australia and Malaysia have a definition for it while New Zealand and Singapore do not define this. A global alignment will help to cover these types of gaps which may lead to confusion within users in different regions of the globe.

A. Related Work

The work proposed on the data privacy matrix is a unique area. Comparing data privacy laws is not a new or ground breaking area of research. There are papers, extensive blogs and articles which have been written comparing different jurisdictions like EU and U.S [1] [2] [3] or APAC regions [4]. A recap of data privacy within the APAC is shown in [5], which highlights the inconsistencies between the countries and a need to have an alignment in data privacy laws.
Some work in the EU is a type of alignment where any member country within the EU follows EU directives however these only apply to these EU countries. Agreements like Safe Harbour were a form of alignment where U.S companies had to provide a similar or better level of protection than the EU enforces.

The closest tool available is the DLA Piper handbook [6] which gives an overview of data protection laws and allows the user to compare two countries out of the 89 countries in their list. The handbook identifies the main legislative source for data privacy in each country, however this is not an extensive list of possible legislation in the country that has an effect on data privacy.
Although this tool names the relevant legislation it does not offer the user a location of where to find them; some are easy to find by a simple web search but others may take a bit longer.

B. Goals

The goal of the data privacy matrix is to create a data privacy reference matrix representing all major cloud-hosting countries in the world. As this tool has a wide reaching user base 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.
The data privacy matrix is designed to provide an easy way to cross reference different trans-national legislation which aligns with a set of predefined domain areas. This will assist a user to see what laws are governing their data wherever in the world it may be located.
By having the matrix available to any user at any time it will

be able to guide them to specific legislation which will help to answer any questions or worries they might be facing. The data privacy matrix can also help clarify if a certain aspect of data privacy means the same thing across the regions around the world.

II. Background

A. The NSA Leaks

In 2013 a former CIA employee and former contractor for the U.S Government Edward Snowden, released classified information relating to numerous global surveillance programs, many of which were run by the NSA and the Five Eyes Alliance. This release of classified information to the public related to the clandestine surveillance program known as PRISM and other information about covert spying operations by the U.S government on its citizens. With media outlets over the world reporting on these developments it became clear that this would have a massive impact on the data privacy debate. Since the leaks the Information Technology and Innovation Foundation (ITIF) and industry-funded think tank that focus on the intersection of technological innovation and public policy, estimated that the leaks could cost cloud computing companies up to $35 Billion in lost revenue [7].

With the fallout from this exposure it forced countries who were using data centres in the U.S 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. [7].
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 U.S centres to another part of the world where the laws were unknown to them.

B. PRISM

The PRISM program was launched in 2007 after the enactment of the Foreign Intelligence Surveillance Act (FISA). PRISM was carried out by the NSA to collect stored Internet communications and use data mining techniques to look for patterns of terrorist or other potential criminal activity within the communications. There were at least nine major U.S 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 [8].
The basic idea behind the program was for the NSA to have the ability to request data on specific persons of interest. Permission is given by the Foreign Intelligence Surveillance Court, a special federal court setup by FISA. There are still questions about the operation of the FISA court and if its actions are in breach of the U.S constitution.

C. Cloud Computing

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, of these participants 95% are using cloud services [9].
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 on the precise number of data centres that Google has; some of them are located in South America, Europe, India, Asia as well in the U.S. [10]. 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 U.S. their data may be subject 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 easily be spoofed, this makes 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.

D. Trans-national Agreements

To protect data privacy within the EU, the data protection directive 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-U.S Umbrella Agreement is a framework to enable co-operation between law enforcement efforts between the EU and U.S 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 [11].
The safe harbour agreement was an important step towards trans-national partnerships. It was set up to allow commercial companies to transfer data from the EU to the U.S and store the data within the U.S. The agreement was enacted in 2000 which 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 U.S was able to self-certify or outsource the certification to a third party, where they must comply with the seven principles in the agreement as well as a set of 15 Frequently Asked Questions (FAQ). The safe harbour principles were an expansion on the original 1980 Organization for Economic Co-operation and Development (OECD) recommendations towards privacy principles for personal data [12]. So providing these two requirements were met, along with the EU Data Protection Directive, Swiss requirements and a $100 yearly fee the company could be part of the safe harbour agreement. This registration method is not stringent and has the possibility for misuse.
However the safe harbour agreement was ruled invalid in October 2015 by the Court of Justice of the European Union (CJEU) following the Schrems case covered later in this section.

E. Privacy Shield

After the invalidation of the safe harbour agreement in late 2015 and two years of deliberation in wake of the Snowden leaks, a draft of the new EU-U.S privacy shield [13] emerged. The draft privacy shield was announced in February 2016 which is an adaption of the safe harbour agreement. There are still some holes in this agreement but it should have some positive impact on restoring a level of trust back into the flow of data between the EU and U.S [14].

III. Legal Cases

Privacy concerns are an ongoing issue that may only get more complicated as the technological landscape evolves. In recent years there have been some important landmark legal cases which reaffirm the need for a project of this calibre.

A. Schrems case

A huge turning point for the data privacy movement came as a result of the efforts by Max Schrems [15], an Austrian PhD student and privacy activist. During his time at Santa Clara University he wrote a term paper on Facebook's lack of awareness of European privacy law. During this research he made 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.
The majority of Facebook users within the EU have their data transferred from Facebook's Irish subsidiary to servers located in the U.S. Mr Schrems made a complaint to the Irish DPA with concerns over his data being stored in the United States. His case was eventually sent to the CJEU, where the Court ruled the safe harbour agreement invalid [16].
This decision put many companies who relied on the safe harbour agreement in a state of limbo and scrambling to find a way to provide alternative guarantees for customers to continue their services lawfully.

B. Google Spain v AEPD and Mario Costeja González

An important case in the privacy area came in 2014 with the Google Spain case, also known as the "Right to be Forgotten ruling" [17]
A Spanish citizen made a complaint against a Spanish newspaper, to the Data Protection Agency in 2010, as well as against Google Spain and Google Inc. The complaint was in relation to the Google search engine showing results regarding having his home repossessed some time earlier which was then resolved but the search results showing the auction notice were still available and now irrelevant. His request was to have all personal information removed from the newspaper and from the Google search [18].
The Spanish Court referred this case to the CJEU where it was ruled in favour of the defendant. The judgement relied on three main points. The most significant was reference to 'Article 12: Right of Access' of the EU Data Protection Directive which states that an individual has the right to ask search engines to remove links with personal information about them, in certain circumstances.

IV. Challenges

Every country has legislation of some kind, whether that be state, national or federal legislation, constitutions or National policies. These are set by the local government to provide a level of protection for its citizens in various ways. Data privacy is no different. This section will cover how these different pieces of legislation can sometimes be more of a barrier for the everyday user of cloud or web services who does not have a mind for the legislative frameworks.

A. Limitations

Within the APAC, EU and U.S countries there is no one size fits all legislation that covers all aspects of data privacy law. A country such as New Zealand have the Privacy Act 1993 [19] 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 [20], Unsolicited Electronic Messages Act 2007 [21], Search and Surveillance Act 2012 [22].
This does not cover the amount of tortuous 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. A great 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 that in some cases have led to suicide. In 2015 New Zealand enacted the Harmful Digital Communications Act 2015 [23] 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.

B. Interpretation

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.
Users of cloud or web services wanting to find out about another countries' laws regarding their data may find it hard to understand the terminology used or misinterpret how the legislation is intended to be used which may lead to confusion.
An example of how this wording can change between jurisdictions is the term which is used to identify the person whom personal data belongs to. New Zealand 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" [24] which refers to any

Control Domain	Control Specification	New Zealand	Australia	China	United Kingdom
Pre Collection Process	Consent is required from the individual involved	- Privacy Act 1993 Section 6 Principle 3	- Privacy Act 1988 Schedule 1, Principle 2	- Consumer Rights and Interests Article 29 - PIP Section 4.2 d - SNIP Article 2	- Data Protection Act 1998 Schedule 2 - DPD Section 30

TABLE I: An example of a control alignment from the Data Privacy Matrix

operation or set of operations performed on the data. Whereas in other APAC countries they specify in the section if it means delete, modify or destruction etc.
These examples again show the necessity for a global alignment, in this case not necessarily legislation itself but how the legislation is worded to limit this range of mixed terminology.

C. Legislative Hierarchy

Legislative hierarchy refers to how the order of laws should be interpreted; this is from the highest form of law in a country to the lowest (usually a local by-law or regulation).
In the APAC countries of New Zealand, Australia, Singapore, Malaysia and China three out of these four countries are relatively similar with regards to where their online legislation is stored and can be found. They are stored on the government websites which is publicly available and holds all other national legislation. Australia, New Zealand and Singapore even have similarities in the layout legislation.
China's legislative hierarchy on the other hand is not as user friendly as its other APAC counter parts for non legal minded people. Firstly the legal hierarchy in China is vastly different compared to somewhere like Australia which has federal and state laws. Some of the online sources for legislation require a subscription for access to the resources, which is not realistic for a user to have a one time look.

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 National People's Congress or the Standing Committee of the National People's Congress then Administrative Regulations by the State Council.
Most countries will have simple names or at least easily recognisable names for legislation for example New Zealand 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.

V. Solutions

The solution this paper proposes is the data privacy matrix. This matrix is a Rosetta Stone like matrix which helps to align data privacy laws throughout APAC, the EU and the U.S. It does this by having a set of seven predefined domains which include a control specification. The Rosetta Stone [25] was a stone uncovered in 1799 with writing inscribed on it in two languages - Egyptian and Greek. These are done in three scripts - hieroglyphic, demotic and Greek.
The first domain is 'Legislative Framework' which includes six 'control specifications'. Next to each control specification it lists the name of the documents relevant to that specification. The document name in the first domain gives the user the full name of the document and a link they can click which will take them to that document.

The privacy matrix directs a user to a specific section, article, schedule or part in the applicable legislation, this reduces the user hunting through government or other websites to find the relevant legislation they need and then directs them to the specific part of that legislation where they can see what the law states. The privacy matrix allows a user to see if there are any similar laws to do with that control within some of the countries located in the APAC, EU or U.S.
An example of the data privacy matrix can be seen in Table I. This example shows a control specification from the pre-collection process domain. It directs the user to many different documents that relate to whether consent is required from the individual involved in the collection. In New Zealand there are three documents identified. The Privacy Act 1993 - which is the legislation, section 6 which in the Act is titled 'Information Privacy Principles' and then to principle 3. By the user following this they can quickly and painlessly find and identify any relevant information relating to consent. The example also shows the names of Australia, China and the United Kingdom which helps the user to see immediately that there is some law around consent in these countries.

A. Data Privacy Matrix Road Map

The data privacy matrix started off as a project which looked at aligning data privacy laws within the APAC region. Out of the APAC countries there were five countries chosen - New Zealand, Australia, China, Malaysia and Singapore, this is because these countries all participate in providing major cloud services. It was a logical choice to look at the alignment of these countries first. The next step is to align the United Kingdom and the USA. For the EU countries there have been four countries chosen- United Kingdom, Sweden, France, Poland, Estonia and Germany. These countries have been chosen as they are among the most influential EU countries. [26] Estonia has been chosen as it is a leader in cybersecurity and e-government.
It was decided at the beginning the data privacy matrix would be at a high level of legislation covering federal legislation that covers an entire country. State and local laws have been left out at this point, but may be introduced at a later time. It

Control Domain	Control Specification	New Zealand	Australia	China	Singapore	United Kingdom
Privacy Body	There is a requirement each company establishes their own privacy officer to ensure the company complies with policy	- Privacy Act 1993 Section 23			- Personal Data Protection Act 2012 Section 11 (3)	

TABLE II: An example of a control alignment from the Data Privacy Matrix with gaps

also does not look at tortious or civil laws as these are not as black and white as the federal legislations.

B. Use Case

A relatively new start up company named 'Data Storage Solutions Group' (DSSG) has a business which offers cheaper and more reliable data storage. They are a local data centre within their residing country of Australia. DSSG have many clients using their services in Australia and word has spread to U.S about the exceptionally reliable service. Within a few months they have thousands of new clients using their data centres to store different forms of data. With all the excess traffic from the U.S, DSSG have decided to open a new U.S 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. Unsure and with a slight lack of U.S law, they turn to the data privacy matrix to give them guidance.
By using the data privacy matrix they are able to quickly compare and align the laws in Australia with the laws in the U.S and avoid any serious repercussions on their business. Luckily thanks to the data privacy matrix DSSG can successfully open their new data centre and maintain their high standard of data privacy protection for storage.

C. Methodology

When developing the data privacy matrix it was clear that it would not be possible to align every law within the intended countries. The first version of the data privacy matrix was a very simple design which did not have the control domain. The DLA handbook was a starting point which allowed for an idea of potential alignment control specifications. As the research progressed over the different countries in the APAC, new additions were made to the list of domain specifications which came from reading other legislation and following those sections which referred to other similar sections or legislation. By the end of the first version we had a better idea of important control specifications that could be further explored to create other control specifications. The data privacy matrix did not have an easy to follow flow to it, so the control domains were introduced to combine similar control specifications. As it turned out these control domains could then be named in a logical order from legislative framework through the steps of collection and storage of data to other areas such as spam and interception of data.

D. Data Privacy Matrix

The data privacy matrix can be seen in Appendix A. This shows two small examples of the data privacy matrix in its current form.
There are four boxes that highlight parts of the data privacy matrix in figure 1.
The box numbered '1' is labelled "Control Domain", this enables the user to look for a broad area, the example shows two of the domains - Legislative framework and Privacy Body.
The box numbered '2' is labelled "Control Specification", allows the user to look for a more specific issue they are wanting to find out about.
The box numbered '3' is highlighting a control specification "There is a requirement to establish a privacy commissioner". The user can look at this specification to identify if there is a legislative requirement for a country to establish some sort of privacy commissioner to over see any privacy issues.
The box numbered '4' is highlighting the direct piece of legislation that will show the user the specific Act and section in New Zealancd to find out the answer to the domain specification outlined in the box numbered '3'.

The first control domain has links to the relevant Acts or documents that are referred to throughout the data privacy matrix which means the user can link to the document without having to spend hours trying to find it.

E. Gaps

The data privacy matrix is not necessarily just for users of cloud or web services, but it also has the possibility to be used by governments to identify gaps within their own legal system.
Table II shows the privacy body control domain with the control specification relating to ensuring a company operating within that jurisdiction has a privacy officer to enforce and attend to any privacy issues within the company. In this example it shows that only New Zealand and Singapore have this requirement outlined in their legislation. This would ideally assist governments in Australia, China and the United Kingdom to identify these gaps within their own legislation and give them an opportunity to align their legislation with the other countries and implement some sort of amendment which would cover this area.
The data privacy matrix also provides other specifications that are being debated and discussed throughout the world. 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 data privacy matrix shows a gap across all of the countries included in the data privacy matrix.

VI. Concluding Remarks

The data privacy rights within cloud and web services are still unclear to users and vendors. There is a need for a global alignment of data privacy laws.
This paper has proposed the data privacy matrix, a Rosetta Stone like matrix which aligns the different data privacy laws across the APAC, EU and U.S in a clear and concise way to help users know the legislation across this trans-national environment.
The data privacy matrix is a new tool that can direct users, vendors and governments towards the current legislation in place in these various regions, helping them to identify any laws that are potentially or currently affecting their data. The data privacy matrix provides the user with a quick and easy way of finding the relevant section within the appropriate document.
In a quickly evolving technological environment that is struggling to keep up with legislating against these technologies and services, it is important that there is an easily accessible way of identifying any gaps that may lead to a potential financial or personal loss of data.

The goals of the data privacy matrix were to create a tool which would include all major cloud-hosting countries. Currently it includes the major players in the APAC, EU and USA. The wording has been made as simple and non technical to accommodate all users, but also adding a definitions page which allows users to see different terminology used between jurisdictions. The last part of the initial goals were to make it publicly available at any time. This is still a work in progress and will hope to be released in the coming months.

It can be seen from the events and technological progress over the last decade that the world is moving closer to a complete digital era, where everything will be done online. The data privacy matrix will help with providing information to users as this evolution happens, meaning users can reference the data privacy matrix and always be aware of where their data will be safe and secure and their privacy adequately protected.

VII. Future Work

The first completed draft of the **DPM!** (**DPM!**) is now completed but there is still more work to do on the data privacy matrix to ensure it is 100% reliable for all users and governments, as legislation is continuously being amended and new pieces put into force, the **DPM!** needs regular updates.
The validation step is vital for the privacy data matrix. This preferably needs to be in the form of a peer review process that involves law and data privacy professionals to contribute by verifying the correct legislation has been referred to, any gaps that have been identified are correct and those gaps actually exist and there is nothing important missing that could be added, whether that be a new control specification, control domain or new piece of legislation.
As this will be based on an ever growing industry there is always the possibility for adding additional content to make it more comprehensive. At present there are only three regions being aligned, the APAC, EU and U.S however this could eventually be extended to cover Africa, South America and Middle Eastern countries.

VIII. Access to Data Privacy Matrix

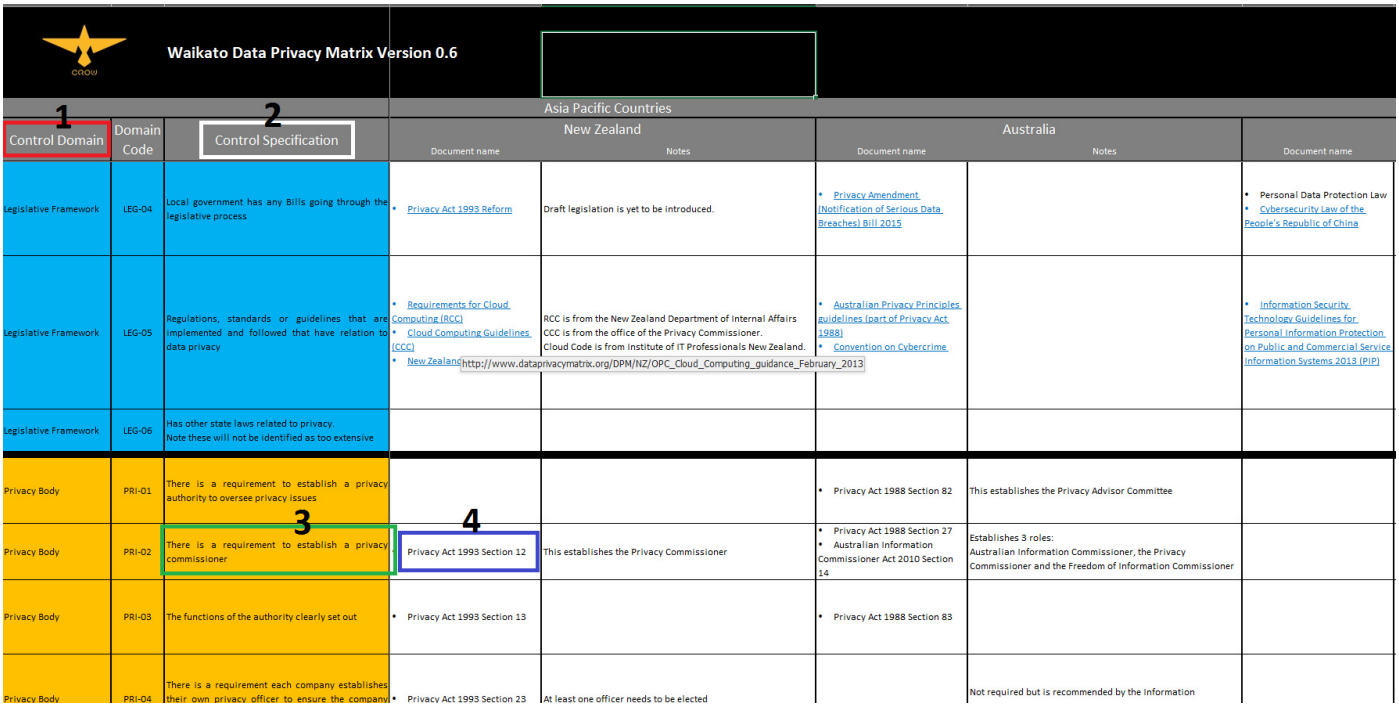
The Appendix shows a snapshot of the current version of the data privacy matrix. The whole document will be available on the website mentioned below after the validation has been completed.
More information and resources can be found at http://www.dataprivacymatrix.org

Acknowledgements

This research is supported by STRATUS (Security Technologies Returning Accountability, Trust and User-Centric Services in the Cloud) (https://stratus.org.nz), a science investment project funded by the New Zealand Ministry of Business, Innovation and Employment (MBIE), Cloud Security Alliance (CSA) (https://cloudsecurityalliance.org/). The authors would also like to acknowledge the expert inputs from Mr John Edwards, the New Zealand Privacy Commissioner, and his colleagues at the Office of the Privacy Commissioner New Zealand, and Associate Professor Wayne Rumbles, Dr Sivadon Chaisiri and Dr Harris Lin from the University of Waikato, New Zealand.

Appendix

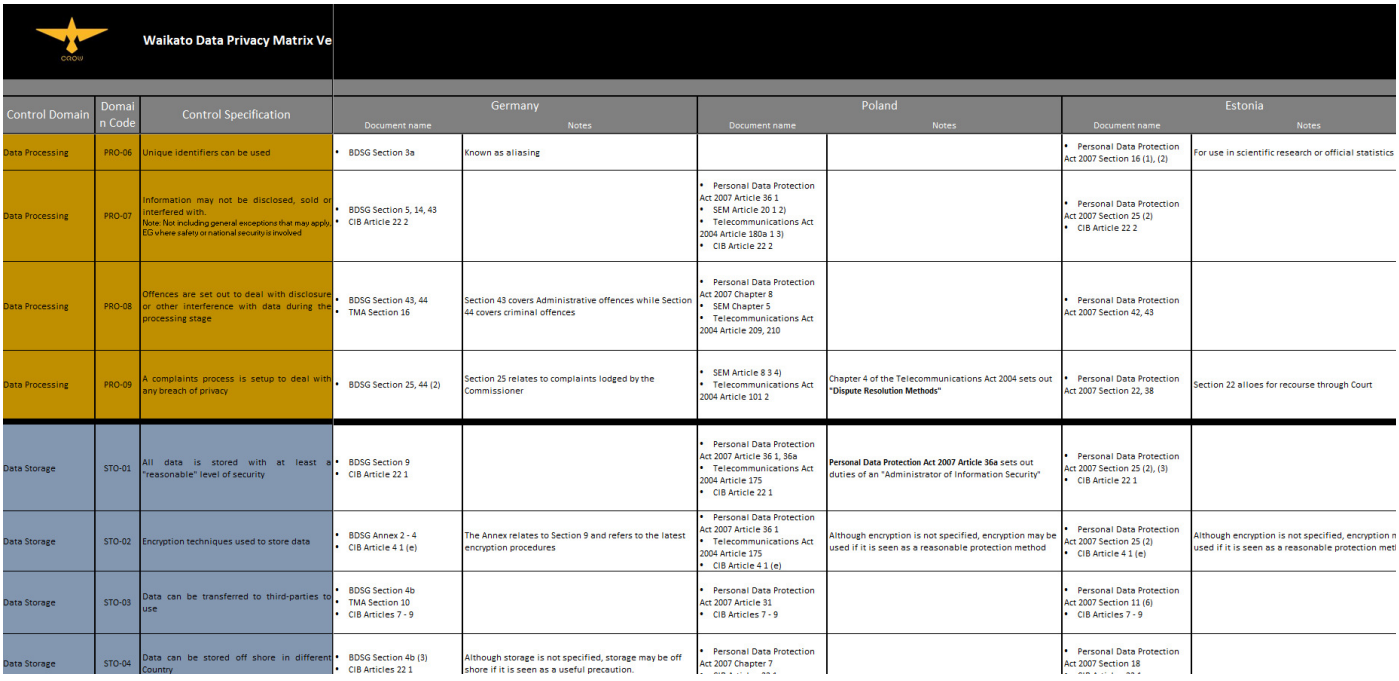
Appendix A



Waikato Data Privacy Matrix Version 0.6

Control Domain	Domain Code	Control Specification	Asia Pacific Countries				
			New Zealand		Australia		
			Document name	Notes	Document name	Notes	Document name
Legislative Framework	LEG-04	Local government has any Bills going through the legislative process	• Privacy Act 1993 Reform	Draft legislation is yet to be introduced.	• Privacy Amendment (Notification of Serious Data Breaches) Bill 2015		• Personal Data Protection Law • Cybersecurity Law of the People's Republic of China
Legislative Framework	LEG-05	Regulations, standards or guidelines that are implemented and followed that have relation to data privacy	• Requirements for Cloud Computing (RCC) • Cloud Computing Guidelines (CCC) • New Zealand	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.	• Australian Privacy Principles guidelines (part of Privacy Act 1988) • Convention on Cybercrime		• Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems 2013 (PIP)
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			• Privacy Act 1988 Section 82	This establishes the Privacy Advisor Committee	
Privacy Body	PRI-02	There is a requirement to establish a privacy commissioner	Privacy Act 1993 Section 12	This establishes the Privacy Commissioner	• Privacy Act 1988 Section 27 • Australian Information Commissioner Act 2010 Section 14	Establishes 3 roles: Australian Information Commissioner, the Privacy Commissioner and the Freedom of Information Commissioner	
Privacy Body	PRI-03	The functions of the authority clearly set out	• Privacy Act 1993 Section 13		• Privacy Act 1988 Section 83		
Privacy Body	PRI-04	There is a requirement each company establishes their own privacy officer to ensure the company	• Privacy Act 1993 Section 23	At least one officer needs to be elected		Not required but is recommended by the Information	

Fig. 1: An example of the Data Privacy Matrix Version 0.6



Waikato Data Privacy Matrix Ve

Control Domain	Domain Code	Control Specification	Germany		Poland		Estonia	
			Document name	Notes	Document name	Notes	Document name	Notes
Data Processing	PRO-06	Unique identifiers can be used	• BDSG Section 3a	Known as aliasing			• Personal Data Protection Act 2007 Section 16 (1), (2)	For use in scientific research or official statistics
Data Processing	PRO-07	Information may not be disclosed, sold or interfered with. Note: Not including general exceptions that may apply, EG where safety or national security is involved	• BDSG Section 5, 14, 43 • CIB Article 22 2		• Personal Data Protection Act 2007 Article 36 1 • SEM Article 20 1 2) • Telecommunications Act 2004 Article 180a 1 3) • CIB Article 22 2		• Personal Data Protection Act 2007 Section 25 (2) • CIB Article 22 2	
Data Processing	PRO-08	Offences are set out to deal with disclosure or other interference with data during the processing stage	• BDSG Section 43, 44 • TMA Section 16	Section 43 covers Administrative offences while Section 44 covers criminal offences	• Personal Data Protection Act 2007 Chapter 8 • SEM Chapter 5 • Telecommunications Act 2004 Article 209, 210		• Personal Data Protection Act 2007 Section 42, 43	
Data Processing	PRO-09	A complaints process is setup to deal with any breach of privacy	• BDSG Section 25, 44 (2)	Section 25 relates to complaints lodged by the Commissioner	• SEM Article 8 3 4) • Telecommunications Act 2004 Article 101 2	Chapter 4 of the Telecommunications Act 2004 sets out "**Dispute Resolution Methods**"	• Personal Data Protection Act 2007 Section 22, 38	Section 22 alloes for recourse through Court
Data Storage	STO-01	All data is stored with at least a "reasonable" level of security	• BDSG Section 9 • CIB Article 22 1		• Personal Data Protection Act 2007 Article 36 1, 36a • Telecommunications Act 2004 Article 175 • CIB Article 22 1	**Personal Data Protection Act 2007 Article 36a** sets out duties of an "Administrator of Information Security"	• Personal Data Protection Act 2007 Section 25 (2), (3) • CIB Article 22 1	
Data Storage	STO-02	Encryption techniques used to store data	• BDSG Annex 2 - 4 • CIB Article 4 1 (e)	The Annex relates to Section 9 and refers to the latest encryption procedures	• Personal Data Protection Act 2007 Article 36 1 • Telecommunications Act 2004 Article 175 • CIB Article 4 1 (e)	Although encryption is not specified, encryption may be used if it is seen as a reasonable protection method	• Personal Data Protection Act 2007 Section 25 (2) • CIB Article 4 1 (e)	Although encryption is not specified, encryption n used if it is seen as a reasonable protection met
Data Storage	STO-03	Data can be transferred to third-parties to use	• BDSG Section 4b • TMA Section 10 • CIB Articles 7 - 9		• Personal Data Protection Act 2007 Article 31 • CIB Articles 7 - 9		• Personal Data Protection Act 2007 Section 11 (6) • CIB Articles 7 - 9	
Data Storage	STO-04	Data can be stored off shore in different Country	• BDSG Section 4b (3) • CIB Articles 22 1	Although storage is not specified, storage may be off shore if it is seen as a useful precaution.	• Personal Data Protection Act 2007 Chapter 7		• Personal Data Protection Act 2007 Section 18	

Fig. 2: General example of the Data Privacy Matrix Version 0.6

REFERENCES

[1] D. Dimov, "Differences between the privacy laws in the EU and the US," January 10 2013, (Last Accessed on 07 April 2016). [Online]. Available: http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/

[2] P. Lee, "How do EU and US privacy regimes compare?" March 5 2014, (Last Accessed on 07 April 2016). [Online]. Available: http://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare/

[3] K. Sandoval, "Privacy laws and international data exchange: Comparing EU and US standards," October 8 2015, (Last Accessed on 07 April 2016). [Online]. Available: http://nordicapis.com/privacy-laws-and-international-data-exchange-comparing-eu-and-us-standards/

[4] G. Greenleaf, "Asia-Pacific developments in information privacy law and its interpretation," *UNSW Law Research Paper*, no. 2007-5, 2007, (Last Accessed on 07 April 2016). [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952578

[5] "Recap of APAC data privacy in 2014," November 3 2014, (Last Accessed on 07 April 2016). [Online]. Available: http://www.infocore.com/insights/data-privacy-recap-of-apac-data-privacy-in-2014.htm

[6] "Data protection laws of the world," (Last Accessed on 07 April 2016). [Online]. Available: https://www.dlapiperdataprotection.com/#handbook/world-map-section

[7] N. Arce, "Effect of NSA spying on us tech industry: $35 billion? no. way more," June 10 2015, (Last Accessed on 03 April 2016). [Online]. Available: http://www.techtimes.com/articles/59316/20150610/effect-of-nsa-spying-on-us-tech-industry-35-billion-no-way-more.htm

[8] 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

[9] K. Weins, "Cloud computing trends: 2016 state of the cloud survey," February 9 2016, (Last Accessed on 06 April 2016). [Online]. Available: http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey

[10] "Google data centres," February 9 2016, (Last Accessed on 07 April 2016). [Online]. Available: https://www.google.com/about/datacenters/inside/locations/index.html

[11] "Questions and answers on the EU-US data protection umbrella agreement," September 8 2015, (Last Accessed on 03 April 2016). [Online]. Available: http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm

[12] "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

[13] G. Maldoff, "We read privacy shield so you don't have to," March 7 2016, (Last Accessed on 04 April 2016). [Online]. Available: https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to

[14] P. Sayer, "Five things you need to know about the EU-US privacy shield agreement," March 1 2016, (Last Accessed on 04 April 2016). [Online]. Available: http://www.computerworld.co.nz/article/594954/five-things-need-know-about-eu-us-privacy-shield-agreement/

[15] "The Schrems decision: How the end of safe harbor affects your FCPA compliance plan," November 12 2015, (Last Accessed on 04 April 2016). [Online]. Available: http://www.globaltradelawblog.com/2015/11/12/the-schrems-decision-how-the-end-of-safe-harbor-affects-your-fcpa-compliance-plan/

[16] L. Mays and S. Maberry, "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

[17] "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

[18] "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

[19] "Privacy Act 1993," 1993, (Last Accessed on 04 April 2016). [Online]. Available: http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

[20] "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

[21] "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

[22] "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

[23] "HarmfulDigital Communications Act 2015," 2015, (Last Accessed on 04 April 2016). [Online]. Available: http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html

[24] "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

[25] "The rosetta stone," (Last Accessed on 28 April 2016). [Online]. Available: http://www.ancientegypt.co.uk/writing/rosetta.html

[26] "EU countries ranked for 'influence potential'," July 29 2009, (Last Accessed on 28 April 2016). [Online]. Available: http://www.euractiv.com/section/future-eu/news/eu-countries-ranked-for-influence-potential/