COMP210 Assignment 2

Privacy of communications and data storage is important to most ICT users. Cryptography is one of the most effective ways to protect data at rest

Cameron McLennan
8168187

TABLE OF CONTENTS

In this essay, I have researched current laws relating to the use of cryptography, and have created a profile of nations showing which inhibit and which encourage privacy protection via the use of various cryptographic techniques. Below, it can be seen that I have tried to the best of my ability to convey each respective country's point of view on cryptography and its use for data protection.

Cryptography law, or Encryption law, is the law that deals with information and the way that is protected both in a static context and when information is in transit. There are four main areas that Cryptography law covers. These four areas being: Export Control Laws, Import Control Laws, Patent Issues, and Search and Seizure. Export Control Laws are the laws that limit the export of current crypto methods of a country to another country. Import laws are the laws that restrict local usage of certain types of cryptography. Patent issues are issues that deal with the intellectual property of the actual cryptographic tools and forms of encryption. The final area, Search and Seizure, usually deals with "criminal constitutional issues regarding under what circumstances a person can be compelled to decrypt data files or reveal an encryption key (*About us - The Wassenaar Arrangement.*)". (*Hg.org)*

The Wassenaar arrangement is essentially a global agreement on export controls, such as how weapons that could be damaging to a country, are transported and transferred from one country to another. All participating countries are all aiming to ensure that the transfers of these cryptographic items does in no way contribute to the enhancement and growth of

military capabilities, and are not diverted to support such capabilities. It has specific measurements and restrictions on what is deemed to be secure enough to be managed by them. From The Wassenaar site itself, it is described as "The Wassenaar Arrangement was established in order to contribute to reginal and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual use goods and technologies, thus preventing destabilising accumulations." (*About us - The Wassenaar Arrangement*.) (*RSA Laboratories - 6.5.3 What is the Wassenaar Arrangement?)*

Below is the Profile of Nations, a collection of nations cryptographic policies and views on the subject. It will display what some of the larger countries from around the world think of cryptography in terms of privacy and how each country prefers to treat cryptography.

The United States of America is one of the great military powers on this planet, and with being one of the most influential countries on earth, they would have to be strict with cryptography exports, imports and usages. For many years, the US didn't approve of export of crypto products unless key size was limited. Due to this, cryptography products were split into two categories; products with strong cryptography and products with weak cryptography. The Wassenaar arrangement essentially guided US to set the below rules on what is weak cryptography. The US set weak cryptography as being something that has a 56 bit key size for symmetric algorithms, has an RSA modulus of size 512 bits, or has elliptic curve key size of at most 112 bits. (*About us - The Wassenaar Arrangement*.) (*Crypto Law Survey - Page 2*. (2013)) (*Hg.org)*

As of January 2000, cryptography export regulation restrictions greatly relaxed, with no import restrictions on cryptography. Any cryptography product can be exported under a license exception unless end users are foreign governments or embargoed destinations, which are: Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, and Taleban-controlled areas of Afghanistan (*Crypto Law Survey - Page 2*. (2013)). There have been legal cases within the United States of America that has really pushed the bounds of what could be deemed "privacy invading", where government agencies, such as the FBI, have demanded that Apple help them crack into an iPhone used by a terrorist. The only way that Apple could have gotten into the phone is by developing software to crack into the device itself, which in turn would have weakened all iPhone security due to how it had to be implemented. A US judge, by the name of Sheri Pym, was the one that legally ordered Apple to create this software for the FBI, but Apple refused. Tim Cook, Apple CEO, was quoted as saying "the order went too far, and would threaten the security of all iPhone users. Bypassing the iPhone's password meant creating a "back door" in its iOS mobile software that could then be used to access every other iPhone. "(*Apple's battle with the FBI leaves lingering questions*. (2017)) (*Hg.org)*

Currently the 5th amendment to the US constitution protects witnesses from being forced to incriminate themselves and there is no law regarding key disclosure in the US, meaning that they do not have to disclose a key to access a device and incriminate themselves. In the past, there has been cases that have had judges telling the criminal to decrypt their device but other cases stating that doing so is violation of someone's 5th amendment rights. (*Crypto Law Survey - Page 2*. (2013) (Karsten, D. (2016)) (*Key disclosure law*. *En.wikipedia.org*.)

The USA is full of people, and with more and more people becoming aware of companies harvesting their data to sell or just having things that they want kept private, people will be starting to encrypt their data. This will create problems in the future for America, and the way that its whole legal system is built with its foundations within The Bill of Rights, will pose problems in the future for events such as the Apple vs FBI event.

The United Kingdom, like many other countries, follows the Wassenaar Arrangement with regards to export controls of cryptography to other EU countries. Transport by "intangible means", such as transport via the internet, is also covered by the regulation. The Open General Export License provides a personal and community license exemption for cryptography goods. This allows export of controlled items to many countries, provided that it is for personal use or is used by others for cryptographic content development. (*Crypto Law Survey - Page 2.* (2013)) (*RSA Laboratories - 6.5.1 What are the cryptographic policies of some countries?)*

In 2015 David Cameron began advocating for limits preventing ordinary people from using end to end encryption that the government couldn't decrypt, and on top of that, the Government introduced a legislation that would ban large tech companies from offering end to end encryption, whereas earlier in the year the UK was encouraging large orginisations to adopt encryption. The Regulation of investigatory powers act of 2000 requires a person to provide the keys to access or decrypt protected information without a court order. If this is not done, one can face prison time of up to two years, or five years should it involve child indecency. First used in 2007, and three people have been prosecuted for refusal to surrender encryption keys. (*Crypto Law Survey - Page 2.* (2013)) Something like this in the United States would not happen due to the fact that they are protected by the 5th amendment, and there being no key disclosure law in place.

Canada is another country who follows Wassenaar regulations, albeit not completely. Exported items by be subject to restriction if they are on the Export Control list. There is open exchange between Canada and the US with regards to importing and exporting cryptography, but any cryptography which is not included in the Export Control List will remain under the US export rules. Canada has a form of key disclosure, which is covered by existing interception, search and seizure and assistance procedures. Canada doesn't currently have any domestic laws or regulations regarding cryptography. (*Crypto Law Survey - Page 2.* (2013))

Back in 1998, "Industry Minister John Manley explained, 'warrants and assistance orders also apply to situations where encryption is encountered — to obtain the decrypted material or decryption keys.'" (*Crypto Law Survey - Page 2.* (2013)) It was also stated that the Canadian government supports industries to use key recovery techniques for stored data. The government also made it an offense to "wrongfully disclose private encryption key information and to use cryptography to commit or hide evidence of a crime." (*Crypto Law Survey - Page 2.* (2013))

There have been two instances of case law in which one had an accused get asked what the passwords were for encrypted drives, but he refused to cooperate. There were no further details given on the outcome of this. The second case was a similar in the fact that part some seized hard drives were encrypted and were required in a court case. An application for a copy of the encrypted files was refused on the grounds of the Crown being unable to exercise its ability to "protect individuals' privacy interest or to prevent further criminal acts from being committed or facilitated when handing over the data." (*Crypto Law Survey - Page 2*. (2013))

Japan follows the Wassenaar arrangement and the General Software Note, with regards to their export of cryptography. Decisions with regards to cryptography are made on an individual case basis. As of the year 1996, whether or not under pressure by the US, for any cryptography export order larger than 50,000 yen, businesses must acquire approval before exporting. (*Crypto Law Survey - Page 2*. (2013))

There are no real domestic laws and regulations in Japan currently with regards to production and use of cryptography, whether it be creation of such software, or usage of any software related to cryptography. The Japanese realize the importance of cryptography for establishing information security in fields such as e-commerce. They encourage the development of cryptography, and network users should be provided with more information about cryptography. (*Crypto Law Survey - Page 2*. (2013))

Australia regulates exports of cryptography through the Defense and Strategic Goods List (DSGL) as of 1999, due to the Wassenaar arrangement. The general technology note is included, which exempts public domain software from controls. Regulation of mass market software is regulated according to limits of the Wassenaar arrangement. There are currently no direct controls for importing of cryptography into Australia, and there aren't really any direct controls for usage of cryptography within Australia. (*Crypto Law Survey - Page 2*. (2013))

As with some other countries, approval is required for software that doesn't specifically contain cryptography but has an interface which can accept cryptography. A section was inserted into the Crimes Act 1914, which requires either decryption of encrypted data or the encryption keys to be released upon a magistrate's order. This order is granted if there is reasonable evidence that a suspect is hiding data that pertains to the case. (*The Australian Cryptography FAQ*. (2017)) (*Crypto Law Survey - Page 2*. (2013))

Australia meets the Defense trade controls (DTC) act of 2012, which is strengthened update from the defense and strategic goods list of 1999. The Defense Trade Controls amendment bill of 2015 came into service in 2016 and essentially combined offense provisions for supplying and publishing DSGL technology from the DTC and brokering DSGL goods and technology. (*Crypto Law Survey - Page 2*. (2013))

For Germany, Export controls are regulated according to the EU regulation and the Wassenaar Arrangement, just like many other countries in this report. Export controls for mass market crypto is limited to the absolute necessary, as stated by the ministry of economic affairs. For mass market crypto exportation, companies can decide whether or not a general license will cover that export. The only exemption to this is if the crypto is exported to a select few countries or if the crypto software has military applications. Exporters must be able to produce documents with details pertaining to exports when requested to. (*Crypto Law Survey - Page 2*. (2013))

There aren't many domestic laws and regulations regarding cryptography in Germany, besides The Amateur Radio Ordinance law, which prohibits amateur radio to "mystify its contents". Germany has the corner points of German cryptography policy, where there is five points. These being that the government does not see the need to restrict the availability of cryptography, and will actively support the secure encryption within Germany. The German government intends to build trust for the use of secure encryption. They also think that the ability for people to create powerful cryptography products is indispensable. While still in support of encryption, the use of cryptography should not hinder the governments interception ability, so development of cryptography is monitored closely. And lastly, the government is a large supporter of international cooperation in cryptography policy. (*Crypto Law Survey - Page 2*. (2013))

Russia is a country that has also gotten on board with the Wassenaar arrangement, like many others in this report. For Russians, in order to import encryption facilities manufactured abroad, one has to first get a license. Exporting of cryptography is under state control, which is tightly managed. Those who wish to import and export cryptography need to have obtained a license from the Mistry of trade. (*Crypto Law Survey - Page 2*. (2013))

Russia has strict domestic laws regarding the use of cryptography. As of the 3rd of April 1995, state organizations and enterprises are required to have a license to use encryption for authentication, secrecy, storage and transmission. Those who use uncertified cryptography do not have to comply to state orders. (*RSA Laboratories - 6.5.1 What are the cryptographic policies of some countries?)*

The Russian Duma recently passed a bill that is expected to pass into law that specifically requires software companies operating in Russia to build workarounds for encryption that would allow the FSB to view any messages sent. (*ISIS' favourite messaging app may be in jeopardy*. (2016)) This means that because there is an available work around for encryption in software produced in Russia, it will be weaker than had that software been produced elsewhere where there was not a rule to put a backdoor into the software to get through encryption.

Italy is another country in that has its export of cryptography regulated according to the EU regulations. As many other countries have done, Italy has signed the Wassenaar agreement. Use of cryptography in Italy is sometimes mandated by law. Personal data that

pertains to health or sexual life of an individual needs to be encrypted, as stated in the Data Protection Act. Transfer of said data also has to remain encrypted if it is being transferred outside of the premises under the same Data Protection Act. Italy also has a law that demands accessibility of encrypted records for the treasury. Italy doesn't have any real push for development in cryptography regulations. (*Crypto Law Survey - Page 2*. (2013))

Again, another country who is in agreeance with the Wassenaar Arrangement. France has signed the Wassenaar arrangement for export controls, but has not signed the general software note. With regards to importing and exporting, importing and exporting to and from countries outside of the EU and the European Economic area is regulated by law no.2004-575 (*Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique | Legifrance*. (2004)) and decree no.2007-663. Import from within the EU and EEA is free, but from other countries is subject to declaration, unless covered by the decree. Export is subject to authorization, unless, again, covered by decree. Failure to comply with those rules is punishable by one or two years imprisonment depending on whether there was no declaration or there was no authorization, and a fine of 15,000 or 30,000 euros respectively.

Use of cryptography is free (law 2004-575) (*Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique | Legifrance*. (2004)) for digital economy trust. Providing of crypto services is subject to regulation. Unless a service is designated by decree that it does not harm security or defense interests, service provision must be declared. The prime minister can stop circulation of cryptography if the supplier does not comply with current regulations, even if supply is free of charge. (*Crypto Law Survey - Page 2*. (2013)) (*RSA Laboratories - 6.5.1 What are the cryptographic policies of some countries?)*

With regards to New Zealand, New Zealand signed the Wassenaar Arrangement, which was completely implemented in 1999. Public domain software is exempt from controls under the general technology note of the Wassenaar Arrangement.

Crypto export was controlled by both the 1966 customs act and the export prohibition regulations of 1953, but ever since October 1996 it has been controlled by Customs and Excise act of 1996. The agency responsible for this is the international security and arms control division of the ministry of foreign affairs and trade.

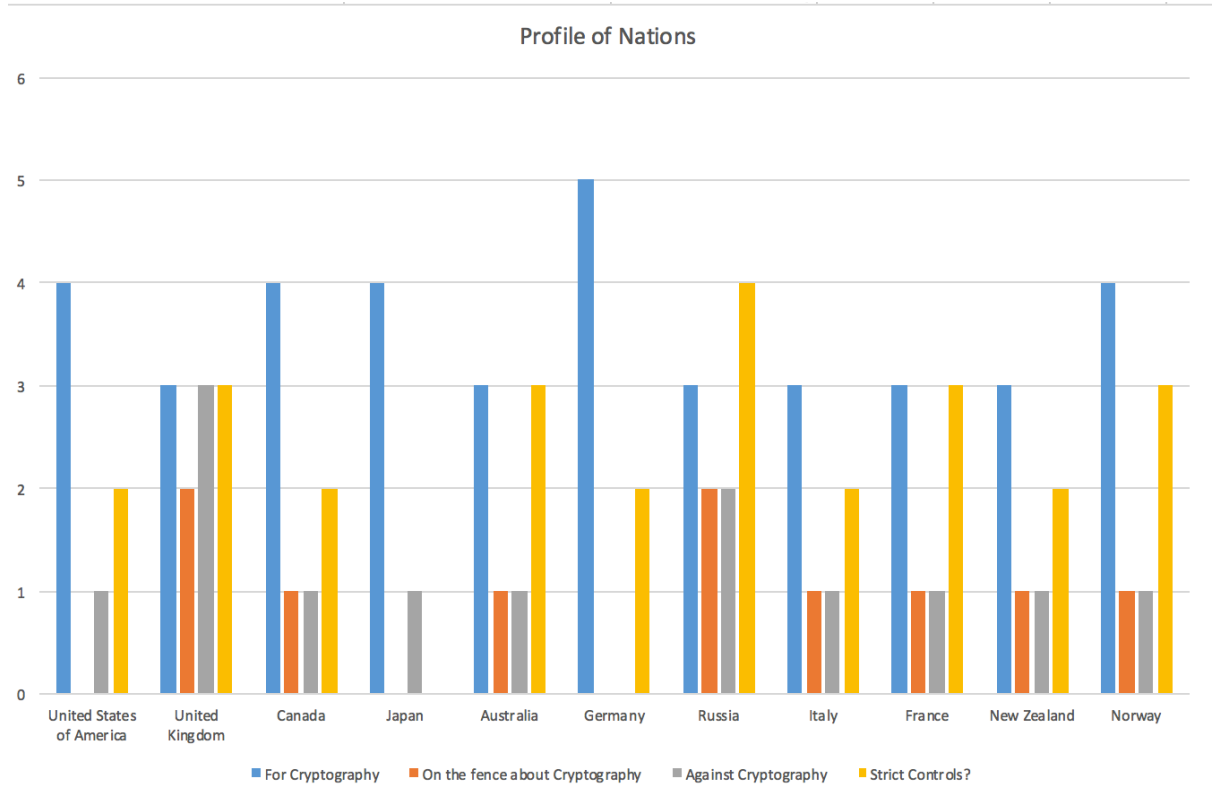
The export regulation does not cover the export of cryptography software by electronic means. As with some other countries, such as Australia, any software that has an interface designed for plugging in cryptography requires approval. Currently there are no domestic laws and regulations surrounding cryptography, and there aren't many developments into cryptography regulations. (*Crypto Law Survey - Page 2*. (2013))

Norway is also a country that has signed the Wassenaar arrangement, which includes the General Software Note. Norway has a policy, by the name of the Norwegian Crypto Policy. This policy is not in favor of mandatory key escrow for private encryption use. The policy is, however, in favor of key escrow for larger companies due to potential data loss should a key

be unable to be recovered or found. The policy also stated that telecom providers, and ISPs may have to provide plaintext to the government, that is if they have access to the plaintext. Should they also have the keys to provide plaintext but not plaintext directly, they may have to provide that instead. Personal data that is transferred electronically that is out of physical control of the data controller must be encrypted or protected in another manner when confidentiality is necessary.

Guidelines have been drawn up for technology and services for military use (e.g defense related products) There are many different products, technologies and services that may not be exported out of Norway without a license from the Ministry of foreign affairs – two lists of items specified by MOFA – list 1 being for defense related products and list 2 including civilian products and and tech that aren't included in list 1 but can still have military uses. These lists are updated regularly. Norway, in general, has a positive attitude on the use of cryptography for protection of its data and economy in general. (*Crypto Law Survey - Page 2*. (2013))

Below is a chart depicting the list of countries talked about, and from my research how much they agree with points on the graph, on a 0 – 5 scale where 0 is not at all and 5 is completely. (The key below is in order of the bars on the graph, should this not come out in colour.)



To summarize what I have found, it seems like some countries are starting to see what is happening in other countries and building up their current laws, or at least looking into building up their laws if they aren't sufficient, whereas some countries are happy to let their

citizens have their data hidden and protected behind encryption. When things like Apple vs FBI happen in one of the most influential countries on the planet, other countries are bound to see what is happening and take preventative measures to protect themselves from such an issue occurring. Things will be changing in the future, and the changes may be quite large. Some countries wouldn't face issues that others face due to how their legal system is set up to protect its citizens, which is where issues do arise when people do wrong, and incriminating evidence is hidden behind encryption. (*The State of Crypto Law: 2016 in Review*. (2017)).

References

About us - The Wassenaar Arrangement. *The Wassenaar Arrangement*. Retrieved 13 May 2017, from http://www.wassenaar.org/about-us/

Apple's battle with the FBI leaves lingering questions. (2017). *CNET*. Retrieved 14 May 2017, from https://www.cnet.com/news/apple-vs-fbi-one-year-later-still-stuck-in-limbo/

Hg.org. Retrieved 13 May 2017, from https://www.hg.org/encryption-law.html

Crypto Law Survey - Page 2. (2013). *Cryptolaw.org*. Retrieved 12 May 2017, from http://www.cryptolaw.org/cls2.htm

Hruska, J. (2015). *UK introduces law to ban civilian encryption, but government policies recommend its use - ExtremeTech*. *ExtremeTech*. Retrieved 21 May 2017, from https://www.extremetech.com/extreme/217478-uk-introduces-law-to-ban-civilian-encryption-but-government-policies-recommend-its-use

ISIS' favourite messaging app may be in jeopardy. (2016). Retrieved 15 May 2017, from https://www.businessinsider.com.au/russia-anti-encryption-telegram-2016-6?r=US&IR=T

Karsten, D. (2016). *A brief history of U.S. encryption policy | Brookings Institution*. *Brookings*. Retrieved 21 May 2017, from https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/

Key disclosure law. *En.wikipedia.org*. Retrieved 15 May 2017, from https://en.wikipedia.org/wiki/Key_disclosure_law

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique | Legifrance. (2004). *Legifrance.gouv.fr*. Retrieved 18 May 2017, from https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id

RSA Laboratories - 6.4 United States Cryptography Export/Import Laws. *Emc.com*. Retrieved 14 May 2017, from https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/united-states-cryptography-export-import.htm

RSA Laboratories - 6.5.1 What are the cryptographic policies of some countries?. *Emc.com*. Retrieved 15 May 2017, from https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/cryptographic-policies-countries.htm

RSA Laboratories - 6.5.3 What is the Wassenaar Arrangement?. *Emc.com*. Retrieved 16 May 2017, from https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/wassenaar-arrangement.htm

Szoldra, P. (2016). *The government's war on encryption is so much larger than unlocking one iPhone*. *Business Insider Australia*. Retrieved 14 May 2017, from https://www.businessinsider.com.au/government-encryption-war-2016-3?r=US&IR=T

The Australian Cryptography FAQ. (2017). *Efa.org.au*. Retrieved 13 May 2017, from https://www.efa.org.au/Issues/Crypto/cryptfaq.html

The State of Crypto Law: 2016 in Review. (2017). *Electronic Frontier Foundation*. Retrieved 17 May 2017, from https://www.eff.org/deeplinks/2016/12/crypto-state-law-end-2016