ASIACRYPT 2014

SPEAKER NOTES: The legal Infrastructure around information security in Asia

Ladies and gentlemen. Good morning.

It is indeed a privilege to be here in this beautiful part of the world where I have not visited before. Thank you for the opportunity to share my thinking on the legal infrastructure around information security with you.

From 2006 I began the habit of rising early to read. Specifically, relating to my interest in the world of information communication technology and human behaviour. The trends that I saw develop from that time were - information warfare, espionage, surveillance, and the lack of privacy.

The Snowden revelations in 2013 confirmed these trends and emphasised that surveillance was the most prevalent, because in most cases, it was an aspect of the other trends.

Linked to my interest in these developing trends, is my interest in law. By this, I mean my interest in the study of law in relation to people and communities.

In simple terms, law may be regarded as the norms of behaviour, that govern people and communities, within a particular place and at a particular time. I think it fair to say that you will make the extension to include not only traditional communities linked to physical places, but also, to online communities such as social media.

Today's communities are like virtual WANS. No longer configured through wired topologies or restricted by physical, geographic boundries. Despite losing its old world jurisdictional basis, law must seek to provide some structure to achieve some degree of certainty in human and commercial relations.

Our world is in a state of flux, the extent of which has never been seen before. The origin of the trends outlined above, I believe, are to be found in three material shifts: (i) the geopolitical shift from West to East; (ii) the shift in power from nation states to individuals; and (iii) the shift in value from real to intangible property.[1]

All these have been brought about by the internet. What then, is the connection to cryptology[2]?

[1] Francis Gurry discusses these in his lecture "Re-thinking the role of IP." http://www.law.unimelb.edu.au/melbourne-law-school/news-and-events/watch-online/francis-gurry

[2] Cryptography (or cryptology; from Greek κρυπτός kryptós, "hidden, secret"; and γράφειν graphein, "writing", or -λογία -logia, "study", respectively is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.

CRYPTOLOGY

Before the internet era, cryptology was concerned solely with message confidentiality –- turning plaintext into ciphertext and back again. It was about keeping secrets mostly, in relation to communications.

During the internet era, cryptology has expanded beyond the concerns of confidentiality to include techniques for ensuring message integrity, authentication and non-repudicaion – the things upon which legal consequences depend, and the things which now concern us regarding the legal infrastructure around information security.

As cryptology evolved to offer not only confidentiality but also the basis for legal certainty and accountability, the laws pertaining to our understanding of how the internet-connected world functioned, also needed to evolve.

In the last 2 decades, we have seen developments in international electronic law driven by a need for certainty and trust. Trust in the world of information security depends upon the confidentiality, integrity and availability of information and information systems.

Your work is critical to trust and to consequence.

Let's look at how the theory of law and the issue of trust have evolved in the light of the legal infrastructure around information security.

LEGAL INFRASTRUCTURE, NATIONAL AND INTERNATIONAL LAW

Firstly**,** to get a grip on the legal infrastructure around information security in Asia, we need to begin with a basic understanding of legal infrustructure in general. We need some idea about how legal systems work.

ASIA, APEC, ASEAN AND SCOPE

References will be made below to ASIA (North, East, South East, West etc) APEC and ASEAN countries. The approach followed is to use reference points and examples only. Clearly the level of detail is restricted given the time available for this talk. It is more important that I equip you with some fundamentals, which will hopefully make it easier for you to understant the bigger picture into which your work fits and possibly inspire new research topics.

NATIONAL (DOMESTIC) AND INTERNATIONAL LAW, REQUIREMENTS FOR STATEHOOD

National law is the domestic law of a state which governs the relationship between a state and its subjects as individuals and entities (like companies). States have the capacity to make and enforce laws in their own spheres but not to impose their laws on other states.

Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Public international law[3] is the body of law which governs the relationship between states and between certain recognised international entities (like the United Nations). It serves as a framework for the practice of stable and organised international relations. Cooperation at an international level is brought about through agreements called treaties or conventions.

The criteria for statehood are described in the Montevideo Convention of 1933,[4] which provides: "The state as a person of international law should posess … a permanent population, defined territory, government and the capacity to enter into relations with other states."

If a state meets these criteria, it is capable of acquiring international legal personality as a sovereign state, and capable of participating in the affairs of the international community[5]. This participation is conducted by the government of a state. A change in government does not usually affect the status of sovereignty but it frequently does affect the national law of a state. Governments are voted into power based on political policy. It is this policy that affects the character of national laws.

Whilst the sources of national law depend upon the history, culture, customs and religions of a state, public international law sources are described in the Statute of the International Court of Justice[6] to include international conventions.[7]

PUBLIC INTERNATIONAL LAW AND CONVENTIONS

An international convention[8] is an instrument that is binding under international law on states, and other entities with recognised legal personality such as the United Nations and the International Court of Justice.

Conventions do not automatically apply to states. Under the general principles of the law of conventions, the act of signing a convention does not automatically make the signatory

[3] Private international law, or conflict of laws, addresses the questions of (1) which jurisdiction may hear a case, and (2) the law concerning which jurisdiction applies to the issues in the case.

[4] Although only 15 Latin American states and the US are parties to the Convention, it is generally accepted as reflecting the requirements of statehood under customary international law.

[5] The rules for the recognition of states is complex and outside the scope of this discussion, except perhaps to mention the status of Taiwan[5], which is not recognised as a sovereign state. This is the result of fairly recent history. The Republic of China, or Taiwan, lost its United Nations seat as "China" in 1971 and was replaced by the Peoples Republic of China. Most sovereign states as members of the United Nations switched their diplomatic recognition to the Peoples Republic of China, recognizing or acknowledging the Peoples Republic of China to be the sole legitimate representative of all China. Despite this, as of 2013, the Republic of China or Taiwan, maintains official diplomatic relations with 21 United Nations member states and the Holy See (Papal State), and informal relations are maintained with nearly all other United Nations members.

[6] Article 38(1).

[7] The other sources are International custom; general principles of law recognised by civilised nations; and judicial declarations and teachings of the most highly qualified publicists.

[8] http://www.uncitral.org/uncitral/en/uncitral_texts.html and https://treaties.un.org/

state a party to that convention. A further act such as ratification or accession is required for the state to be bound by the convention. Legislation may also be required to be promulgated into the national law of a state in order for the terms of the convention to be implemented within the state[9].

In summary, conventions in international law can become part of a sovereign state's national law.

Model laws[10] also, can also become part of a sovereign state's national law although these operate differently from conventions.

NATIONAL (DOMESTIC) AND MODEL LAWS

A model law is created as a suggested pattern for law-makers in sovereign states to consider adopting as part of their national legislation. If adopted, such a law is the same as any other national (domestic) law passed within the state by the government in power.

So, who is responsible for drafting model laws?

The United Nations Commission of International Trade Law (UNCITRAL) is the core legal body of the United Nations system in the field of international trade law. To date, UNCITRAL has been responsible for one convention and two model laws which have shaped the modernisation and harmonisation electronic commerce.[11]

These are the foundations for the legal infrastructure around information security, even, here in Asia.

The UNCITRAL Model law on Electronic Commerce[12] was adopted in June 1996.[13]

It seeks to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce.

The UNCITRAL Model law on Electronic Commerce was the first legislative text to adopt the fundamental principles of non-discrimination (a document would not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form), technological neutrality and functional equivalence.

[9] UNCITRAL monitors ratifications of conventions and enactments of UNCITRAL. It is also advisable to consult the United Nations Treaty Collection for authoritative status information.
[10] http://www.uncitral.org/uncitral/en/uncitral_texts_faq.html#model
[11] While the ambit of the UNCITRAL's activities is wide, relating to diverse aspects of trade law, for the purposes of this paper, we will look only at its activities that relate to Electronic Commerce. Activities include arbitration, sale of goods, securities, insolvency, payments and transport of goods.
[12] http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf
[13] The important additional article 5 *bis*, dealing with incorporation by reference, was adopted in 1998.

The functional equivalence principle lays out the criteria under which electronic communications may be considered equivalent to paper-based communications. In particular, it sets out the specific requirements that electronic communications need to meet in order to fulfil the same purposes and functions that certain notions in the traditional paper-based system like, "writing," "original," "signed," and "record" seek to achieve.

Technological neutrality, non-discrimination and functional equivalence are the founding elements of modern electronic commerce law.

In addition to the above, the UNCITRAL Model law on Electronic Commerce establishes rules for the formation and validity of contracts concluded by electronic means, for the attribution of data messages, for the acknowledgement of receipt, and for determining the time and place of dispatch and receipt of data messages. All these rules relate to integrity and the functions of cryptology.

Key to our understanding of information security is that a reliable assurance of integrity is required to assess originality. The criteria for assessing integrity include whether the information has remained complete and unaltered, demonstrating for example the service provided by a hash function.

With regard to legal admissibility and evidential weight, courts will have regard to the reliability of the manner in which the data message was generated, stored or communicated, the reliability of the manner in which the intrgrity of the information was maintained, and the manner in which the originator was identified.

All these reference cryptology as do the requirements for the retention of data messages namely, that the information is accessible so as to be usable for subsequent reference, retained in the format generated, sent, received, enables identification of the origin and destination and date and time sent and received. All these requirements are functions of cryptology.

No definition is provided for “signature” (article 7) in this Model Law, which simply states that where law requires a signature, that requirement is met in relation to a data message if a method is used to identify a person and to indicate that person’s approval of the information in the message, and that the method is as reliable as appropriate in the circumstances. This too references possible cryptographic services but is not specific with regard to Publik Key Infrastructure or other kinds of signature, a matter clarified in the second Model Law in 2001.

Please note that exclusions to the recognition of electronic formats exist in the Model Law, and in the national law versions of electronic transcations laws adopted by the various states.

It is also important to note that the parties to an electronic transaction can vary certain of the provisions by agreement and that consent on a number of issues is necessary. Article *bis 5* which provides for the incorporation by reference which was added to the Model Law in 1998 is important for all of the requirements of electronic transactions law. In simple terms, it means that information accessible via a URL becomes part of a binding legal agreement. Here too, all of the requirements are functions of cryptology.

According to UNCITRAL, legislation based on the Model Law on Electronic Commerce[14] has been adopted in 61 States in a total of 136 jurisdictions. In Asia[15], these include Australia, China, Hong Kong, India, Malaysia, Philipines, Singapore, Thailand, Viet Nam, New Zealand and the Lao Peoples Democtatic Republic. Notably, not Japan, Korea or Taiwan.

The UNCITRAL Model Law on Electronic Signatures was adopted in July 2001[16].

It aims to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures.

It builds on the principle in the Model Law on Electronic Commerce with respect to the fulfilment of the signature function in an electronic form, with the result that legislation based on this Model Law may recognise both digital signatures based on cryptology (such as public key infrastructure) and electronic signatures using other technologies (biometrics, signature pads).

The UNCITRAL Model Law on Electronic Signatures is based on the fundamental principles common to all UNCITRAL texts relating to electronic commerce, namely non-discrimination, technological neutrality and functional equivalence.

It establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures as well as basic rules of conduct that may serve as guidelines for assessing duties and liabilities for the signatory, the relying party and trusted third parties intervening in the signature process.

Key provisions include a definition for “electronic signature” which means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message. A “certificate” means a data message or other record confirming the link between a signatory and the signature creation data.

The requirement for signature is specified as follows:

[14] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html
[15] In describing Asia, we consider a selection of Asian, APEC, ASEAN and countries, and Australia and New Zealand.
[16] http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

Where law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

An electronic signature is considered to be reliable if the signature creation data are linked to the signatory and to no other person; at the time of signing, under the control of the signatory and no other person; any alteration to the electronic signature, made after the time of signing, is detectable ; and where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration to the information after the time of signing, is detectable.

This Model Law on Electronic Signature also provides for the matter of trust in relation to certification service providers stating that the quality of hardware and software will be a factor in assessing trust.

Legislation based on the UNCITRAL Model Law on Electronic Signatures has been adopted into national law by 29[17] states in Asia including China, India, Thailand and Vietnam. The other Asian countries that adopted the Uncitral Model Law on Electronic Commerce have retained the former provision, lacking the recognition and certainty provided in the second Model Law.

To summarise, the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures are model laws which provide an agreed basis upon which sovereign states may elect to adopt the suggested provisions into their national legal systems, each through its own individual national legislative process.

In Asia, China, India, Thailand, Vietnam have adopted both Model Laws into their national legislation. The effect of this is that it adds certainty to the national laws of each of these states. It does not deal with the issue of the rules that apply between these states. A convention is required to achieve the latter.

INTERNATIONAL CONVENTIONS (TREATIES, AGREEMENTS)

We turn our attention now from the Model Laws to Conventions as international agreements.

The Convention on the Use of Electronic Communications,[18] was adopted in November 2005.

It aims at facilitating the use of electronic communications in international trade. It does so by providing assurance that contracts concluded and other communications exchanged electronically are as valid and enforceable as their traditional paper-based equivalents.[19]

[17] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_status.html
[18] http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

The Electronic Communications Convention builds upon earlier instruments drafted by the Commission, in particular, the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures.

As with these Model Laws, the Convention is intended to strengthen the harmonisation of the rules regarding electronic commerce and foster uniformity in the national enactment of the Model Laws. It sets forth the three fundamental principles of electronic commerce legislation namely, non-discrimination, technological neutrality and functional equivalence.

The Convention applies to all electronic communications exchanged between parties whose places of business are in different states when at least one party has its place of business in a contracting state.[20]

It sets out criteria for establishing the functional equivalence between electronic communications and paper documents, as well as between electronic authentication methods and handwritten signatures. It specifies the time and place of dispatch and receipt of electronic communications.

According to UNCITRAL, the status of contracting states[21] at the time of preparing this paper is as follows:

China signed in 2006, Philipines signed in 2007, Republic of Korea signed in 2008 and Sri Lanka signed in 2006. There has been no ratification, accession, approval, acceptance or succession by any of these states.

The Russian Federation signed in 2007 and accepted the Convention in 2014. It came into force in 2014.[22] Singapore signed in 2006, ratified the Convention 2010 and in it came into force 2013.[23]

---

[19] It also removes formal obstacles in international trade law treaties such as the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the "New York Convention") and the United Nations Convention on Contracts for the International Sale of Goods.

[20] Art. 1. Note also that under Art. 2. contracts concluded for personal, family or household purposes, such as those relating to family law and the law of succession, as well as certain financial transactions, negotiable instruments, and documents of title, are excluded from the Convention's scope of application. It may also apply by virtue of the parties' choice.

[21] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html

[22] Upon acceptance, the Russian Federation declared: 1. In accordance with article 19, paragraph 1, of the Convention, the Russian Federation will apply the Convention when the parties to the international contract have agreed that it applies; 2. In accordance with article 19, paragraph 2, of the Convention, the Russian Federation will not apply the Convention to transactions for which a notarized form or State registration is required under Russian law or to transactions for the sale of goods whose transfer across the Customs Union border is either prohibited or restricted; 3. The Russian Federation understands the international contracts covered by the Convention to mean civil law contracts involving foreign citizens or legal entities, or a foreign element.

[23] Upon ratification, Singapore declared: The Convention shall not apply to electronic communications relating to any contract for the sale or other disposition of immovable property, or any interest in such property. The

REGIONAL PRESENCE FOR UNCITRAL IN ASIA AND THE PACIFIC

A regional centre for UNCITRAL in Asia and the Pacific has been established in Incheon in the Republic of Korea in order to enhance international trade and development, provide assistance and coordinate activities between states in the region and UNCITRAL.[24]

Council of Europe's Convention on Cybercrime[25]

The Convention was adopted by the Council of Europe in November 2001. The Council, is an international organisation promoting cooperation between the European states in matters relating to legal standards, human rights, democratic development, the rule of law and cultural co-operation. It is an entirely separate body from the European Union and should not be confused with it.

The Convention on Cybercrime, also known as the Budapest Convention, is the first international treaty seeking to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations.

The Convention aims principally at harmonising domestic criminal substantive law (what) in the area of cyber-crime, providing for domestic criminal procedural law powers (how) necessary for the investigation and prosecution of offences committed by means of a computer system or evidence in electronic form, and setting up a fast and effective regime of international co-operation.

9 offences are defined in the Convention. These are illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

In 2006 the Additional Protocol to the Convention on Cybercrime came into force requiring states that have ratified the additional protocol to criminalise the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivated by racism or xenophobia. Reflecting the human rights and freedom of speech focus.

As at October 2014, 44 states had ratified the Convention. While the countries of Asia are not members, certain have ratified the Council's Convention of Cybercrime. These include Australia and Japan. Canada and the United States of America, also non-members of the

---

Convention shall also not apply in respect of (i) the creation or execution of a will; or (ii) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney, that may be contracted for in any contract governed by the Convention.

[24] Recent events have been held in New Deli, Beijing, Seoul, Sydney, Kyoto, Macau, Hong Kong, Colombo, Canberra.

[25] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

Council of Europe, but important members of the Asia Pacific Economic Cooperation have also ratified the Conventions.

We need now, to move away from the over-arching and interpretive electronic transactions laws to information technology - specific legislation.

INFORMATION COMMUNICATION TECHNOLOGY SPECIFIC LAW

Parallel with the period of international cooperation in electronic transactions law, 3 major trends developed in information communication technology - specific law. These are:

- Access to information, meaning access to information held by the state;
- Surveillance, meaning interception and monitoring by states at a national level and by organisations at the employer level; and
- Privacy and personal information.

These three trends are inter-related and involve the delicate need to balance rights between the government of a state and the subjects of the state.[26] This is a vertical legal relationship founded on the moral and political philosophy of the social contract

Social contract is a theory that addresses the questions of the origin of society and the legitimacy of the authority of the state over the individual. Social contract arguments typically hold that individuals have consented to surrender some of their freedoms and submit to the authority of the ruler, in this case, the government acting for the state, in exchange for protection of their remaining rights. While social contract theory dates back as far as the 15th century, it is in my view as relevant today.

ACCESS TO AND FREEDOM OF INFORMATION LAWS

Access to or freedom of information laws[27] allow access by the public to data held by national governments, and sometimes to other non-government organisations . They establish a 'right-to-know' legal process by which requests may be made for government-held information, to be received freely or at minimal cost, barring standard exceptions, which typically involve law enforcement and individual rights, such as privacy.

Freedom of information laws exist to promote government accountability and transparency in policy making, administrative decision-making and government service delivery by providing a legal framework for individuals to request access to government documents, including what information government holds about them, and to seek

[26] Some jurisdictions accord similar rights and obligations to juristic and to natural persons. This paper will not detail both two aspects.

[27] Over 90 countries around the world have implemented some form of freedom of information legislation, starting with Sweeden in 1766.

correction of that information if they consider it wrong or misleading (privacy rights mirror this). Ideally, the community can be better informed and participate more effectively in a nation's democratic processes.

What then is the relevance of freedom of information laws to crypology?

Broadly speaking these laws cater for certain kinds of information to which rights and duties attach. An accountable entity will need to know what information it has and be able to classify and handle the information appropriately with respect to confidentiality, integrity and availability, electronic transactions law, legal compliance and risk.

In Asia, Australia, India, Japan, Malaysia (Selangor and Penang states), New Zealand, Pakistan, the Peoples Republic of China, Republic of China (Taiwan), South Korea and Thailand all have freedom of information laws.

In Hong Kong while there are no laws specifically enacted to guarantee the freedom of information, the government of Hong Kong promulgated a "Code on Access to Information" in 1995 to serve a similar purpose. This code, like other internal regulations of the Government, was not legislated by the Legislative Council and has a minimal legal status.

EXAMPLES OF FREEDOM OF INFORMATION LAWS IN ASIA

India has the Right to Information Act 2005,[28] an "Act to provide for …. the right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability in the working of every public authority,…", because India recognises that "democracy requires an informed citizenry and transparency of information … vital to its functioning and also to contain corruption and to hold Governments and their instrumentalities accountable …[29]"

Access to information law always entails some basis for refusing or limiting the right of access. For example, in the Taiwan Freedom of Government Information Law, restrictions exist on making government information available to the pulic, where the information is classified by law as a national secret, prohibited by law, required to maintain confidentiality, may obstruct law enforcement or result in injury to life.

Restrictions such as this clearly demonstrate the other side of the legal relationship between the government acting for a state and subjects of the state. While individuals have a right to government information, governments have an obligation and a duty to

[28] http://rti.gov.in/rti-act.pdf

[29] Interestingly, this Act has a requirement for records (ISO 15489) to be "computerised."

ensure the safety and security of the state and its subjects[30]. In seeking to achieve this, it is acknowledged that some level of surveillance is necessary.

As surveillance is a limitation of privacy, we will first take a look at privacy.

PRIVACY AND DATA PROTECTION LAWS

As surveillance has increased, brought on by increased terrorism and cybercrime, not to mention nation state surveillance, so too has the need to push back against surveillance by increasing privacy protections.

There is no absolute definition for privacy, partly, because it is an issue so closely related to custom and national history. One of the better explanations I have come across and that is reflected in national laws, particularly, those with written constitutions, is that it involves the "right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose. [31]"

This understanding of privacy in the sense of personal preferences is in my view, distinct from another aspect of privacy which is better understood through use of the term 'personal information', meaning information which on its own, or together with other information has the ability of identifying a particular individual. It is this kind of information now so freely available in electronic form that enables all manner of new criminal activity, from identity theft through to credit card fraud, to which the issue of cryptology is so relevant.

To limit the scope of this discussion for present purposes, we will focus on privacy in relation to the Asia Pacific Economic Cooperation[32].

The Asia-Pacific Economic Cooperation (APEC) is the world's largest regional economic group. It consists of 21 diverse economies which straddle the Pacific Ocean.

The APEC Privacy Framework aims to promote a consistent approach to information privacy protection across APEC member economies.[33] The Framework Principles and

[30] This government – individual legal relationship is mirrored at a lower level between organisations and individuals as employees(or contractors). Not all state laws include organisations in the duty to make information available to individuals.

[31] Yael Onn, et al*., Privacy in the Digital Environment,* Haifa Centre of Law and Technology, (2005) pp. 1 - 12

[32] http://www.apec.org/

[33] http://www.apec.org/ APEC has 21 member economies. In Asia, these include Australia, People's Republic of China, Hong Kong China, Indonesia, Japan, Republic of Korea, Malaysia, New Zealand, Papua New Guinea,Republic of the Philippines, the Russian Federation, Singapore, Republic of China (Taiwan), Thailand and Vietnam.

implementation guidance[34] focus on protections for personal information, prevention of unnecessary barriers to information flows, the enablement of uniform approaches to the collection, use and processing of data, and facilitation of domestic and international efforts to promote and enforce information privacy protections.

The APEC Cross-border Privacy Enforcement Arrangement provides a framework for privacy regulators to cooperate, and to seek information and advice from each other in enforcement matters. Linked to the Enforcement arrangements is the Data Privacy Pathfinder initiative which involves the development and implementation of a Cross-border Privacy Rules which are intended to assist affected entities meet the APEC requirements.

The APEC-Cross-border Privacy Rules System is the first pan-global framework that has been endorsed by regulators and that addresses data flows between the United States and other APEC Member Economies[35]. Cooperation agreements such as this do not fall within the structure of domestic or international law discusses earlier. They are nevertheless binding agreements founded on consensus.

In addition to the cross-border flows of personal information, the privacy laws of most countries that regulate this issue include principles that provide for transaprent and accountable management, the right of the data subject to remain anonymous, unsolicited communications and marketing, use and disclosure of personal information, other identifiers, quality or integrity, access and correction, and most importantly, security – without which privacy cannot exist.

Once again, the relevance of this body of internatiol law to cryptology is confidentiality, integrity and availability. It is also inseperable from electronic transaction and communications law.

SURVEILLANCE, MONITORING AND INTERCEPTION LAWS

According to Edward Snowden, this slide shows a map of the undersea phone and internet cables spied on by British Intelligence Government Communications Headquarters.

I think it is important to point out that what was generally accepted in democratic societies as necessary surveillance in terms of social contract theory, pre-dates what we now know as the total drag-net surveillance,[36] involving the mass surveillance of entire

[34] This is Consistent with the Organisation for Economic Co-operation and Development's (OECD) Privacy Guidelines. See http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[35] http://www.truste.com/blog/2014/05/07/japan-joins-apec-cross-border-privacy-rules-system/#sthash.SJpEDI70.dpuf

[36] Global surveillance refers to the mass surveillance of entire populations across national borders. Its roots can be traced back to the middle of the 20th century, when the UKUSA Agreement was jointly enacted by

populations across national borders, undertaken by states as revealed by Edward Snowden.

The origin and purpose of surveillance law lies in the right and the duty of a state and other entities to manage security and risk.

At a government level, it concerns the safey and security of the state and law enforcement powers. It relates most specifically to terrorism, cybercrime and the errosion of the tax base. Secrecy is a primary consideration at state level.

At an organisational level, surveillance is related to organisational policy, legal compliance and risk. Confidentiality is the primary consideration for organisations. Particularly given the value of intellectual property in the information age.

Both secrecy and confidentiality are functions of cryptology.

At both the state and the corporation level, two aspects of surveillance law are important, telecommunications law and broadcasting law.

TELECOMMUNICATIONS AND BROADCASTING LAW (VOICE, DATA, LIVE AND STATIC)

Historically, there is a distinction between how voice and data have been, and still are, regulated. It means that there is a distinction between how the state and organisations can lawfully access information. The general principles of the law of evidence require that evidence is among other things, legally obtained. If not legally obtained, it may not be admissible in a court of law. It is also important to understand the distinction because unauthorised access is a criminal offence.

Laws dealing with surevillance and access to information also make a distinction between 'live' communications (telephone conversations and communications in transit over the internet) and data at rest (stored) communications.

The laws of some countries have converged their telecommunications and broadcasting laws to reflect the technological reality of different content being offered on the same platforms. For example, voice over internet protocols. Complexities arise though in the many and inconsistent definitions applied internationally to the body of surveillance and access law.

---

the United Kingdom and the United States, which later expanded to Canada, Australia, and New Zealand to create the Five Eyes alliance. Eventually, this resulted in the establishment of a global surveillance network, code-named "ECHELON", in 1971. Its existence, however, was not widely acknowledged by governments and the mainstream media until the global surveillance disclosure by Edward Snowden triggered a debate about the right to privacy in the digital age. A secret treaty is a treaty between nations that is not revealed to other nations or interested observers. An example would be a secret alliance between two nations to support each other in the event of war.

Surveillance and access laws usually begin with a general rule prohibiting surveillance of live communications and access to stored communications. These are followed by exclusions to the general rule which cater for lawful surveillance and access.

Let's look at Australia, which offers a good example of this. Please note that in addition to the issues already introduced, Australia is a federal state (India is another example). I will illustrate below how this adds to the complexity of surveillance law.

In Australia, the Commonwealth Telecommunications (Interception and Access) Act 1979[37] protects the privacy of Australians by prohibiting the interception of communications or access to stored communications (email, SMS and voicemail). The focus of the legislation is to protect the privacy of communications, where "communication" is defined to include a conversation and a message, whether in the form of speech, music or other sounds, data, text, visual images, or signals and any combination of these.

The Act sets out exceptions to these prohibitions to permit law enforcement and security agencies to obtain warrants to intercept communications, obtain warrants to access stored communications and authorise the disclosure of telecommunications data on the basis of national security or law enforcement.

The Commonwealth Surveillance Devices Act 1999[38] governs the use of surveillance devices by Australian Government agencies. Under this Act, an eligible Australian government agency can apply for a warrant to use a surveillance device to investigate a relevant offence. Interestingly, a "data surveillance device" means any device or program capable of being used to record or monitor the input of information into, or the output of information from, a *computer*, and specifically excludes an optical surveillance device.

A "listening device" means any device capable of being used to overhear, record, monitor or listen to *a conversation or words spoken* to or by any person in conversation, …'

An "optical surveillance device" means any device capable of being used to record visually or observe an activity, …

A "tracking device" means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.

A "surveillance device" means a data surveillance device, a listening device, an optical surveillance device or a tracking device; or … a combination.

These definitions illustrate the complexity and confusion I mentioned earlier. They also illustrate a failure to maintain technological neutrality suggested in the model laws and conventions.

[37] http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/
[38] http://www.austlii.edu.au/au/legis/vic/consol_act/sda1999210/

In addition to this, in Australia, at a Australian State and Federal level, we see for example, the Workplace Surveillance Act 2005 of New South Wales,[39] which prescribes the way in which employers can legitimately use camera, computer and tracking surveillance to monitor an employee while at work. In the Australian Capital Territory, the Workplace Privacy Act 2001,[40] largely covers the same ground as the New South Wales legislation. In Victoria, however the Surveillance Devices Act 1999,[41] prohibits the use of optical and listening devices in certain circumstances. Two Australian states, Western Australia and South Australia, have no S tate privacy laws. While there is no consistency between the Australian State laws regarding the convergence of voice and data, some include computer and mobile phone surveillance to means software and equipment that monitors or records the "information" input or output and other activity such as sending and receipt of emails and accessing websites, and this, means 'data' as opposed to 'voice'.

In short, the requirements for lawful access in Australia, a country not regarded by the European Union as having an 'adequate' privacy regime, are challenging. Regretably, these challenges are repeated across the world.

ASIA SUMMARY [42]

When referring to political rights and civil liberties, the Freedom House Freedom on the Net Report[43] categorises the following Asian countries as free:

Australia, for its highly effective development of a range of cyber-related legislation, in particular the Criminal Code Act[44] (unauthorised access, modification or imparement with intent to commit a serious offence) and for development of a voluntary code of conduct for ISPs (the iCode[45]).

Japan, which has demonstrated a clear understanding of its vulnerabilities in cyberspace and what needs to be done to address them. In June 2013, the Japanese Government adopted the Cybersecurity Strategy, which is focused on building cyber resilience and provides a solid foundation for future cyber efforts.

Philippines, where there is very limited internet regulation. Only one law, the Anti-Child Pornography Act of 2009, places restrictions on online content. The country has a strong Bill of Rights, and ISPs are generally uncooperative when it comes to releasing information to government agencies.

---

[39] http://www.austlii.edu.au/au/legis/nsw/consol_act/wsa2005245/

[40] http://www.legislation.act.gov.au/a/2011-4/current/pdf/2011-4.pdf

[41] http://www.austlii.edu.au/au/legis/vic/consol_act/sda1999210/

[42] https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014/ASPI_cyber_maturity_2014.pdf

[43] https://freedomhouse.org/report/freedom-world/freedom-world-2014#.VHz45KSUcfk

[44] http://www.austlii.edu.au/cgi-bin/download.cgi/au/legis/cth/consol_act/cca1995115

[45] http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative

New Zealand, Vanuatu, Tonga and *Samoa* are also free.

The following countries are "partly free":

Cambodia because its cyber-related legislation is generally undeveloped and most regulations are implemented through ad hoc and non-binding internal circulars and enforced inconsistently.

India, which has some cyber-specific and cyber-related legislation, but that legislation has been used haphazardly and in some cases has granted significant interception and censorship powers.

Indonesia, which has enacted some cyber-specific and cyber-related legislation, including the 2010 TIPITI (cybercrime) Act, but it's not clear that those laws are systematically enforced.

Malaysia, because while its organisational approach has been strong, its supporting legislation is generally vague.

South Korea, which has a strong catalogue of cyber legislation and regulation, along with an active critical infrastructure cyber policy.

Thailand, where cyber legislation and regulation are largely a work in progress.

Singapore, which has successfully implemented legislation, such as the Computer Misuse and Cybersecurity Act, to prevent and respond to cyber issues, including cybercrime and hacking.

The following countries are "not free":

China, based on it's cyber-related legislation which is generally focused on domestic surveillance and information control—specifically, the Law of Guarding State Secrets,[46] and the Security Management Procedures in Internet Accessing.

Myanmar, where the Computer Science Development Law[47] (1996) criminalises the use of a computer network to undermine state security, community peace or national unity or to distribute state secrets, among other actions. The Wide Area Network Order (2002) and the Electronic Transactions Law (2004) both build upon the 1996 law and are products of the period of military rule and censorship within the country.

North Korea has little domestic cyber infrastructure and highly limited internet connectivity. Legislation appears to be limited to governing military operations, content censorship and limiting access.

[46] http://www.chinawuliu.com.cn/?pgv_ref=404
[47] http://www.burmalibrary.org/docs6/Computer_Science_Development_Law.pdf

MECHANISMS THAT SUPPORT LEGAL INFRASTRUCTURE

Mandatory compliance with law is best demonstrated through the adoption of standards, codes and frameworks. There are many of these, including security, evidence, privacy and records management. They should be considered as part of the legal infrastructure around information security because, even in the absence of law, liability can arise where a standard establishes reasonable behaviour.

REGULATORY UNIVERSE

The 'regulatory universe' refers to the laws that apply to a particular entity. This includes, a body of general law, such as tax, that applies broadly, and a body of industry specific law that applies to a vertical sector, such as health and consumer law. The term 'law' refers to primary and to subsidiary legislation and includes, the common law, statute law, regulations, ordinances, by-laws, edicts and the like.

All of these are included in the legal infrastructure around information security, because of the functional equivalence of electronic law and because almost all of them have their own specific requirements relating to the confidentiality, integrity and availability of information.

SUMMARY

In summary, for the purposes of this discussion, the legal infrastructure around information security comprises conventions and other international agreements involving cooperation, national law,[48] the law of contract, standards, codes and best practice frameworks.

CLOSURE AND HOT TOPIC RESEARCH

In closing, we need also to ask again what the connections are for you as cryptologers - what does all this mean to you?

From my side, your work makes trust possible in the virtual world, you have a chance to shape the future, you can fight for good over evil.

My challenge to you, is to consider current aspects of life that point to the future. My clues for you are that you look at the games that children play, research in areas outside of cryptology, and study crime – follow the money.

Mapping these 3 things to the infrastructure around information security that I have shared with you today may yield some interesting outcomes.

[48] There are of course other areas of law, by way of example, private international law, which fall outside of the scope of this discussion, but to which the principles outlined in this paper apply. Reference the case of Julian Assange as an Australian citizen, alleged to have committed a crime in Sweden, and currently granted diplomatic asylum by Ecuador.

I wish you well and thank you for your interest in being here.

[i]

[i] Other references include:
Richard Hall, Empires of the Monsoon.
Robert D Kaplan, The Revenge of Geography.
Niall Ferguson, Civilization.