Journal of South Pacific Law
Volume 10 2006 - Issue 1

SOUTH PACIFIC COMPUTER LAW: PROMOTING E-COMMERCE IN VANUATU AND FIGHTING CYBER-CRIME IN TONGA

STEPHEN E. BLYTHE[1]

ABSTRACT

Vanuatu and Tonga have enacted different types of computer laws. Vanuatu's Electronic Transactions Act ('ETA') is designed to increase the reliability and integrity of E-commerce transactions. The ETA provides for legal recognition of electronic records and electronic signatures and allows them to be used to comply with statutory mandates pertaining to: original documents; written form; delivery; retention; and ink signatures. The ETA includes contract formation rules relating to attribution, acknowledgement of receipt, and time/place that an electronic message has been sent/received. In order to increase the authenticity and accuracy of electronic messages, the ETA established a compulsory system of licensing of Certification Authorities ('CA'), the verifiers that an electronic message has been sent by a specific party and that the message has not been altered since it was transmitted. In order to be licensed, a CA must meet stringent requirements pertaining to knowledge of electronic signatures and computer information systems. A CA is generally liable to its subscribers or relying third parties for erroneous information contained in certificates it has issued, with some exceptions. On the other hand, an internet service provider is generally not liable for information contained in the electronic messages it disseminates, with some exceptions. Vanuatu's E-Business Act ('EBA') allows foreign entities to use Vanuatu as a tax haven by renting an E-commerce website without having to establish a formal corporation. The Kingdom of Tonga enacted the Computer Crimes Act ('CCA') which prohibits these activities: tampering with another's computer or obtaining information from it; interfering with another's computer data or computer system; and trafficking in illegal computer devices. Substantial procedural powers are granted by the CCA to law enforcement authorities. In looking for ways to improve the computer laws of these nations, Vanuatu and Tonga can learn from one another. Vanuatu is in need of a computer crimes law which prohibits computer tampering and violation of security of computer information; Tonga has such a law—the CCA—and Vanuatu can consider it. Tonga is in need of an electronic transactions statute which provides for the legal recognition of electronic records and electronic signatures; Tonga may also want to enact a law giving tax advantages to foreign entities that rent a Tonga-based website for use in international E-commerce transactions. Vanuatu already has such statutes—the ETA and the EBA—and Tonga can consider them.

OBJECTIVES OF THE ARTICLE

The objectives of this article are to: (1) introduce the reader to the South Pacific nations of Vanuatu and Tonga; (2) explain the role of electronic signatures, cryptology, public key infrastructure, and Certification Authorities; (3) analyse Vanuatu's Electronic Transactions Act and E-Business Act; (4) analyse Tonga's Computer Crimes Act; and (5) make recommendations for improvement of the computer laws of these two nations.

REPUBLIC OF VANUATU

The Republic of Vanuatu ('Vanuatu') entails more than 80 islands in a chain lying in the South Pacific Ocean, about 75% of the distance on a line drawn from Hawaii to Australia. More than sixty of the islands are inhabited. The land area is slightly larger than the U.S. State of Connecticut. British and French immigrants settled in these islands in the nineteenth century. From 1906 until the islands achieved their independence in 1980,[2] they were ruled jointly by Great Britain and France[3] and were referred to as the New Hebrides.[4] Ninety-four percent of the citizens of Vanuatu are of Melanesian ethnicity. More than 15% of the nation's population (206,000) live in the capital city of Port Vila on Efate Island.[5]

Vanuatu's Economy

Eighty percent of the population of Vanuatu make their living on small farms; the major products are copra, coconuts, timber, beef, cocoa, root extracts and kava. Offshore financial and banking services are another source of income; Vanuatu has more than 2,000 registered firms in this sector.[6] The country is well known as a tax haven for expatriates.[7] Tourism is the fastest growing industry and now accounts for more than 40% of Gross Domestic Product.[8] More than 50,000 tourists went to Vanuatu in 2004, most of them coming from Australia and New Zealand. During the 1990's, economic growth was tepid. Economic development has been rather hamstrung by the scarcity of export products, the continual problem of natural disasters (including earthquakes and tsunamis[9]) and disadvantageous distances to foreign markets and between the islands of the country. To achieve more economic development, the government has begun to target more growth for the livestock farming and tourism industries.[10] The government's efforts seem to be paying dividends: in real terms, Vanuatu experienced an economic growth rate of 3.2% in 2004.[11] Over the long run, E-commerce may also become a positive influence on the economy. In order to stimulate its development, the government of Vanuatu enacted several statutes pertaining to electronic transactions. Two of those statutes comprise one of the focal points of this article.

KINGDOM OF TONGA

The Kingdom of Tonga ('Tonga') consists of an archipelago of 169 islands, 36 of which are inhabited. Two-thirds of the population lives on its main island, Togatapu, and almost all citizens of Tonga are of Polynesian ethnicity.[12] Twenty-five percent of Tonga's population—34,000 persons—live in the capital city of Nuku'alofa on Togatapu island.[13] Once referred to as the Friendly Islands, Tonga lies about two-thirds of the distance between Hawaii and Australia. Its total land mass is about 4 times the area of Washington, D.C., U.S.A. Tonga became a kingdom in 1845 and a constitutional monarchy in 1875, and is currently the only monarchy in the Pacific region. Although Tonga came under British control in 1900, it regained independence in 1970 and is now a member of the United Nations.[14] In 2005, Tonga became a member of the World Trade Organization.[15]

Tonga's Economy

Two-thirds of the exports of Tonga are agricultural products: squash, coconuts, copra, bananas, vanilla beans, cocoa, coffee, ginger and black pepper.[16] The number-one cash crop is pumpkin squash; this crop was brought in from outside in 1987 and comprises 96% of the exports purchased by Japan. Tonga's over-emphasis on pumpkin squash as a cash crop can be risky, however; in 2002, Tonga's harvest of that item was reduced due to international price competition.[17] Tonga's economy was also shocked in recent years by the East Asian financial crisis and three typhoons which hit the islands during 1998-2001. The unemployment rate is 13%.[18]

Nevertheless, Tonga has been experiencing an increase in its Gross Domestic Product. In addition to agriculture, the government of Tonga is also beginning to nurture other sources of economic growth.

Promotion of tourism, development of the fishing industry, and upgrading of the nation's communication and transportation infrastructure are examples.[19] Tourism especially seems to hold promise for the country; the annual number of arrivals has been in excess of 33,000.[20] Other more bizarre ideas for economic development have often been advocated in recent years, but with little success.[21] Tonga continues to depend upon the remittances of the one-third of its citizens currently living overseas, most notably in New Zealand, Australia and the United States.[22]

An event of September, 2005 brought the government of Tonga to the edge of bankruptcy by early 2006. That event was a massive increase in pay given to striking government workers. The pay increases were enormous, amounting to 60-80% per worker.[23] Tonga's Finance Minister has forecast a huge deficit in the government's budget for the 2006-07 fiscal year. The deficit threatens to have a detrimental impact on Tonga's economy; it could lead to high inflation, a reduction in foreign trade, more unemployment and less creation of new jobs, and a diminishment in the quality and quantity of government services. The Minister hopes that remittances from expatriate Tongans will be increased so that the government's health services do not have to be significantly reduced.[24]

ELECTRONIC SIGNATURES, CRYPTOLOGY, PUBLIC KEY INFRASTRUCTURE AND CERTIFICATION AUTHORITIES

Electronic Signatures

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law.[25] An electronic signature may be defined as 'any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with the intent to authenticate a writing.'[26] There are many forms of electronic signatures; examples include 'a name typed at the end of an e-mail message, a digitized fingerprint, a digitized image of a handwritten signature that is attached to an electronic message, a retinal scan, a pin number, or a digital signature.'[27] One type of electronic signature—perhaps the most sophisticated—is the digital signature.[28] In the Utah statute, digital signatures were given legal recognition, but other types of electronic signatures were not.[29] Although the Utah statute provides for relatively more security in electronic transactions, its technological-exclusivity is burdensome and overly-restrictive. Forcing users to employ digital signatures gives them more security, but this benefit may be outweighed by the digital signature's disadvantages: more expense, lesser convenience, more complication and less adaptability to technologies used in other nations, or even by other persons within the same country.[30]

In drafting an electronic transactions law for Vanuatu, its creators apparently decided to give a preference to the electronic signature which affords the greatest reliability and security—the digital signature.[31] However, despite the fact that Vanuatu recognizes the security advantages afforded by the relatively greater sophistication of the digital signature, the digital signature was not granted a monopoly. Unlike the Utah statute, Vanuatu allows other types of electronic signatures to be employed. This technological open-mindedness is commensurate with a global perspective and allows parties in Vanuatu to more easily consummate electronic transactions with parties from other nations.[32]

Digital Signatures: Three Aspects

If the parties to an electronic transaction employ a digital signature, that decision will have these effects: (1) adoption of asymmetric cryptology; (2) utilization of public key infrastructure ("PKI"); and (3) interaction with a Certification Authority.[33]

In order for a digital signature to attain the same legal status as an ink-on-paper signature, asymmetric key cryptology must have been employed in its production.[34] Such a system employs double keys—one key

is used to encrypt the message by the sender, and a different, albeit mathematically-related, key is used by the recipient to decrypt the message.[35] The sender has a private key, known only to her,[36] used to generate the digital signature, and the recipient uses the public key, often available online, to verify that the proper party created the message and that it has not been altered during transmission.[37] This is a very good system for electronic transactions, since two stranger-parties, perhaps living far apart, can confirm each other's identity and thereby reduce the likelihood of fraud in the transaction.

In order to use this cryptology for electronic 'signing,' a person must first apply for issuance of a pair of keys—a private key and a related public key.[38] A prospective subscriber of a Certification Authority ("CA") requests the CA to confirm her identity. After verification of the applicant's identity, payment of fees and compliance with other requirements, the new subscriber will be issued the private key which corresponds to the public key contained in the Certificate. The Certificate confirms the identity of the subscriber to the world and will be placed in a public repository, most often the CA's website.[39] Whenever the subscriber digitally signs a message, the CA confirms the signature of the sender and informs the recipient of the encrypted message which "public key" is necessary to decode the message.[40] At that point, the recipient is able to access the public key which is used to decrypt the sender's message.[41]

VANUATU'S ELECTRONIC TRANSACTIONS ACT

Purposes

The Electronic Transactions Act[42] ("ETA") was enacted on 12 September 2000[43] and went into effect on 6 November 2000.[44] Its purposes are to: (1) to help Vanuatu become known as an 'international business centre;' (2) to increase E-commerce by enhancing the integrity and security of electronic transactions;[45] (3) to recognize the legal validity of electronic documents and electronic signatures as *bona fide* alternates for paper documents and ink signatures; (4) to increase the confidence of the general public in electronic transactions; (5) to help create a 'legal and business infrastructure' which is essential to the achievement of secure electronic transactions;[46] and (6) to regulate E-commerce transactions, but also to encourage E-commerce development through the operation of free market forces, and to achieve as much self-regulation of the E-commerce industry as possible.[47] The government of Vanuatu has stated that it used the

E-commerce law of the Commonwealth of Bermuda as a model for the ETA.[48]

E-Government

The ETA does not mandate any agency of the government to use electronic documents.[49]

However, if the Minister[50] gives notice in the *Gazette* that a named agency will henceforth 'receive and process' electronic records pertaining to specifically-named matters, then the government becomes obligated at that point to accept and use electronic documents as an alternative to paper documents.[51]

ETA Inapplicable in Some Situations

Electronic documents are unacceptable substitutes for: (1) paper wills and other documents of testamentary disposition;[52] (2) paper documents which convey or transfer real property;[53] and (3) paper documents pertaining to any category of 'transactions, persons, matters or things' as specified in an order of the Minister.[54]

Selected Definitions

The ETA defines twenty-four terms; two of them are presented here.[55]

Accredited Certificate (hereinafter 'Certificate'): a Certificate issued by an accredited certification service provider which confirms the identity of the Certificate holder and verifies the electronic signature of that person.[56]

Authorized Certification Service Provider (hereinafter 'Certification Authority' or 'CA'): a licensed person who is authorized to issue Certificates pursuant to
ETA s 20(20).[57]

Legal Recognition of Electronic Records

Mere Fact of Electronic Form Insufficient to Avoid Recognition

No denial of legal recognition, accuracy, 'admissibility or enforceability' will be allowed based on the mere fact that: (1) the information is in electronic form; or (2) is referenced in an electronic record which purportedly results in such legal effect.[58]

Electronic Records Can Comply With Requirement to Be 'In Writing'

If a law or statute requires information to be in writing to be recognized, or characterizes information as mandated to be in written form, the electronic form will suffice if: (1) it is "accessible;" and (2) it can be retained for use at a later time.[59]

Electronic Records Can Comply With Delivery Requirement

If a law mandates that information must be delivered to a person, that requirement will be deemed met if the information is in the form of an electronic record, and: (1) the sender of the electronic record requires the receiver to acknowledge it; and (2) the receiver acknowledges the receipt of the electronic record.[60] This will hold regardless whether the law creates an affirmative obligation for delivery, or the law warns of resulting effects if the delivery is not made.[61]

Electronic Record Can Comply With Signature Requirement

If a law mandates the affixation of a person's signature on a paper document, this will be met with an electronic record provided: (1) some means is employed to identify the person and to show that she 'intended to sign or otherwise adopt' the electronic record's information; and (2) the means used is reliable, in consideration of the reason for creation of the electronic record or the communication of it, or any 'relevant agreement.'[62] This will be the case regardless of whether there is an affirmative duty to sign, or the law provides deleterious results if a person fails to sign.[63]

Electronic signatures which are supported by a Certificate issued by an accredited CA will definitely comply with a law's requirement for a signature on a paper document.[64] However, an electronic record meeting these requirements will not be refused 'legal effect, validity, and enforceability' merely because: (1) it is not an E-signature; or (2) it is not supported by a Certificate.

Electronic Records Can Comply With Original Requirement

If a law mandates that an original paper document must be presented in order to meet a legal requirement, or if a law requires that a paper document must be stored in its original form, that mandate is met if: (1) there is a 'reliable[65] assurance' that the electronic document, from the time of its creation until the present, has not been altered;[66] and (2) if required to be presented, the information contained in the electronic record will be an accurate representation of the original.[67] This rule holds regardless of whether there is an affirmative duty for presentation or retention in the original form, or the law dictates consequences if the original is not retained or presented.[68]

Electronic Records Can Comply With Retention Requirement

If electronic records are mandated by law to be stored, that mandate will be complied with by the storage of records in electronic form, provided: (1) the information is accessible and can be stored for reference at a later date; (2) the format used in the electronic form is identical to the one in which it was 'generated, sent or received,' or the format is a correct depiction of that information; and (3) the location and date of the transmission and reception is also stored.[69]

Admissibility of Electronic Records and Evidential Weight Granted to Them

In a court of law, the rules of evidence shall not be construed in a manner that will refuse to admit an electronic record into evidence: (1) merely because of its electronic form; or (2) if it is the 'best evidence' available, merely because it is not in its original form.[70]

Factors to consider in determination of the evidential weight to be given an electronic record include: (1) the degree of trust and reliance that can be given the electronic record, taking into account the means of generation, storage and communication; (2) whether the electronic record's integrity has been maintained since it was created, i.e., the trustworthiness of the record and whether there is assurance that it has not been altered; (3) the means of identification of the sender; and (4) other relevant factors.[71]

Rules Pertaining to E-Commerce Agreements

Contract Formation

In the absence of a contrary agreement between the parties, a contractual offer and acceptance may be in electronic form.[72] In communication between the sender and the receiver as they negotiate a contract, declarations or other statements shall not be denied legal effect merely because they are in electronic form.[73]

Attribution

An electronic record may be assumed to have been sent from a particular sender if: (1) the record was sent as a result of the sender's acts; (2) the record was sent as a result of the sender's agent's acts; or (3) the record was sent from the sender's computer system.[74]
Attribution of an electronic record may be proven by any number of methods, including the reliability and integrity of a computer system's security system which indicates the party who sent a message.[75]

Acknowledgement of Receipt

The following rules are applicable if either: (1) the sender has requested the receiver to acknowledge receipt of the message; or (2) the parties have agreed that an acknowledgement is to be sent from the

receiver to the sender.[76]

1. If the parties have not agreed as to the form or the method of the acknowledgement, then the acknowledgement may be given by: (a) any form of communication of the addressee, including automated communication; or (b) any conduct of the receiver that is 'reasonably sufficient' to indicate reception.[77]
2. If the sender states that the electronic message requires an acknowledgement, then the message is assumed never to have been sent until the sender receives the acknowledgement.[78]
3. If the sender has not stated the message is conditional until receipt of acknowledgement, and no acknowledgement has been received by sender within the specified time or the time agreed to (or, if no time had been specified or agreed), then after a 'reasonable time,' the sender: (a) may inform the receiver that no acknowledgement has been received, and may specify a future time certain for its receipt; and (b) if the acknowledgement referred to in (a) is not timely received, then the sender, after notice to the receiver, may act as though the message had never been sent.[79]
4. When the sender receives an acknowledgement from the receiver, the sender may assume that the message has been received, but this assumption does not also necessarily mean that the message received is identical to the one that was sent.[80]

Assumed Time and Place of Sending and Receiving

Unless the sender and the receiver have agreed to the contrary, an electronic message is assumed to have been sent when it enters a computer system not under the control of the sender.[81]
Unless the sender and the receiver have agreed otherwise, the time of receipt is ascertained using the following rules. If the receiver has pinpointed a specific computer system the message should be sent to, receipt is assumed to occur when it enters that specific computer system; or, if the message is sent to one of the computer systems under the receiver's control, but it is not the specific one that was requested, then receipt is assumed to occur when the receiver first becomes aware that the message has arrived at that computer system; or, if the receiver has not designated a computer system for the message to be sent to, receipt is assumed to have occurred when it enters a computer system belonging to the receiver or that fact comes to the attention of the receiver.[82]
Unless the parties have a contrary agreement, then the message is assumed to have been sent from the sender's place of business, and received at the receiver's place of business.[83]

Electronic Signatures

Certified E-Signatures Definitely Comply With Signature Requirement

An electronic signature which is confirmed by a Certificate issued by an accredited CA will definitely meet the requirements of ETA s 11(1)(a) and (b).[84]

Criteria Required for Issuance of a CA's Licence

In order to become a CA, an application must be filed with the Minister in charge of telecommunications.[85] The application must be made on the official form which is provided by the Minister and the application fee must be paid.[86] The licence will be issued by the Minister if she finds

that: (1) the applicant has the requisite 'knowledge and expertise' necessary for the issuance of Certificates; (2) the applicant has the 'technical capabilities' necessary for the provision of Certificates; and (3) meets other criteria to be determined by the Minister.[87]

The Minister will give notice in the *Gazette* to the general public whenever a new CA has been licensed and is authorized to issue Certificates.[88]

Criteria Required for Revocation of a CA's Licence

If the Minister is of the opinion that a CA is no longer is qualified to be a CA,[89] then the Minister will so inform the CA: (1) of her intention to revoke the CA's licence; (2) the reasons for the revocation; and (3) that the CA should submit a written statement within fourteen days justifying why the licence should not be revoked.[90] Whereupon, the CA's statement will be considered by the Minister, and a decision regarding revocation will be made within seven days after receipt of the statement.[91] If the Minister decides to revoke the licence, publication will be made in the Gazette, and the revocation will become effective on the date stated in the notice.[92]

Recognition of Foreign CA's

Realizing that E-commerce is an international phenomenon, the Republic of Vanuatu grants reciprocal recognition to foreign CA's and foreign-issued Certificates. Under the ETA, foreign-licensed CA's are allowed to apply for a Vanuatu CA license. If the license is approved, Certificates issued by the foreign CA will have the same legal rights as Certificates issued by domestic CA's.[93] After publication of public notice, payment of the fees, and compliance with the other criteria, the Certificates and the CA's are treated as if they were domestic in origin.[94] The 'other criteria' are: (1) in the case of Certificates, whether the criteria they met when they were issued abroad are substantially equivalent to the criteria required of Certificates in Vanuatu; and (2) in the case of CA's, whether the criteria they met when they were licensed abroad are substantially equivalent to the criteria required of CA's in Vanuatu.[95]

The Minister may, of course, revoke the recognition of foreign CA's or foreign Certificates if she later finds that either the CA, or the Certificate, no longer meets the criteria. The Minister's procedure regarding revocation of a foreigner's Vanuatu-issued CA licence (and of a Certificate originally issued abroad that was previously recognized in Vanuatu) is the same as for the revocation of a domestic party's Vanuatu-issued CA license.[96]

The Certificate Holder May Use a Pseudonym

It is acceptable for a CA to issue a Certificate to a subscriber whereby the subscriber lists an assumed name on the Certificate, instead of the subscriber's real name.[97] In such a situation, the CA will keep the true identity of the subscriber on file and will ordinarily not reveal it to third parties. However, if the subscriber is accused of the commission of a computer crime involving the Certificate, the CA is obligated to disclose the subscriber's personal information, including her name, to the law enforcement authorities if they request it.[98] In that situation, the CA must keep a record of the information given to the police and inform the subscriber at once.[99]

Liability of the CA

The CA is liable to relying third parties for: (1) the truthfulness of all information contained in the Certificate as of the issue date, unless a contrary statement appears on the Certificate; (2) its assurance that

the subscriber held the private key (the signature creation device) on the date of issuance, which corresponds to the public key (signature verification device) listed or identified in the Certificate; and (3) if the CA generates both the private key and the public key, assurance that the two keys function together in an acceptable manner.[100]

There is no CA liability if: (1) a relying third party either knew, or should have known, that the Certificate had been revoked;[101] (2) the subscriber or subscriber's agent provided false information in the application for the Certificate, the false information appears on the Certificate, and the CA can show that it was diligent[102] in its attempt to verify the information given by the applicant or the agent;[103] or (3) the CA has listed limitations in the Certificate on how it can be used (which may include the maximum financial value of transactions that the Certificate can be used for[104]), and these limitations have been communicated to relying third parties, and the actual uses exceeded the limitations expressed in the Certificate.[105]

Computer Security Methods

Encryption Devices

It is acceptable for a person in Vanuatu to use any encryption device so long as the person came into possession of it in a lawful manner.[106] However, the Minister is authorized to promulgate regulations pertaining to the 'use, import, and export' of such devices, and to prevent the export of encryption devices altogether or to restrict their export.[107]

Data Processing Security Standards

In order to maintain the privacy of personal information, the Minister is authorized to issue regulations for data processing of said information, regardless of the information's country of origin.[108] Such regulations may include: (1) voluntary adoption of secure methods by data processors; (2) publication in a register of the names of data processors who have voluntarily adopted the higher standards of information security; (3) the foreign countries to which the high standards apply; and (4) the different standards applied to information originating in various countries.[109] Data processors who have voluntarily agreed to comply with the said standards must do so.[110] If they fail to do so, it is a criminal offence; the maximum punishment is six months' imprisonment, 1 million Vatus,[111] or both.[112]

Liability of Intermediaries

General Rule: No Liability

An intermediary[113] is not civilly or criminally liable for the content of a message if the intermediary was not the creator of the message, and: (1) the intermediary did not know that dissemination of the message would be grounds for liability; or (2) the intermediary did not know any related facts or circumstances which would have made it reasonable to suspect there was liability; or (3) the intermediary has complied with the ETA s 27 procedure if the intermediary has become aware of the existence of a civil or criminal penalty, or became aware of facts or circumstances which should have led the intermediary to conclude there was a reasonable likelihood of liability.[114]

There is no affirmative duty on the part of an intermediary to monitor any electronic message, information, or record in order to be able to ascertain whether there may grounds for liability.[115] However, the intermediary is responsible for carrying out any contractual responsibilities it has to its

customers, and is responsible for general obedience to the law.[116]

Liability for Defamatory Information

If the intermediary definitely knows that information it is transmitting is defamatory, it must immediately: (1) stop transmitting that information; and (2) inform the client that it will no longer provide a service to transmit that information.[117] Furthermore, the intermediary must inform the Minister or the law enforcement authorities at once regarding the defamatory information and the name of the client the information emanated from.[118]

In many situations, however, the intermediary will not definitely know that the information is defamatory. However, if the intermediary is aware (or should be aware) there is a likelihood the information is defamatory, the intermediary must immediately: (1) obey the Code of Conduct described in ETA s 28 if said Code applies to it; and (2) inform the Minister.[119] Whereupon, the Minister may order the intermediary to: (1) remove the information and cease to transmit it; (2) stop providing all services to the party that originated the objectionable material; or (3) stop providing all service to the person that originated the objectionable material, with respect to that category of material.[120]

The intermediary is immune from any legal liability for any actions taken when it knows the material is defamatory, or when it responds to the order of the Minister in cases where there is a reasonable belief that the material is defamatory.[121]

Intermediaries' Code of Conduct

The Minister may ask an organization representing a group of intermediaries (or 'E-commerce service providers') to draft a Code of Conduct and to submit it to the Minister.[122] If the Minister approves it, the Code of Conduct will be published in the *Gazette* and will be applicable to all those entities specified in the notice.[123]

If no organization represents a group of intermediaries, or that organization has not responded to the Minister's request to draft a Code of Conduct, then the Minister may draft it and publicize it in the *Gazette*.[124]

The Code of Conduct may include the following: (1) types of services to be provided; (2) types of customers permitted to use the service; (3) types of electronic information permitted; (4) the impact of the Code of Conduct upon the contractual rights of customers; (5) information required to be disclosed by intermediaries (e.g., name, address, E-mail address, and registration information); (6) utilization of a 'quality accreditation mark' indicating that the intermediary follows the Vanuatu Code of Conduct; (7) actions to be taken if the intermediaries' customers send 'spam' via E-mail; (8) electronic business activities which are prohibited by Companies Act or the International Companies Act; (9) publication of any material which is illegal under the laws of Vanuatu; (10) customer complaint procedures; and (11) dispute resolution procedures, including electronic ones.[125]

Intermediaries must comply with an approved Code of Conduct.[126] The first time the Conduct of Conduct is violated, the Minister will send a written warning to the firm. The warning may also include an order to make a correction in behaviour or to cease the behaviour.[127] If the party persists in the violation, the intermediary's maximum punishment is a fine of 100,000 Vatus for each day that the violation continues.[128]

Authorization to Promulgate Regulations

The Minister is empowered to issue regulations containing details for the effective implementation of the ETA.[129] Any party violating the regulations may be fined up to 50,000 Vatus.[130]

VANUATU'S E-BUSINESS ACT

The E-Business Act[131] ('EBA') was enacted on 12 September 2000 and became effective on 6 November 2000.[132] Its purpose is to regulate[133] E-commerce websites based in Vanuatu which have been rented by international business firms looking for a tax haven.[134] The EBA creates an Internet Free Trade Zone whereby individuals and firms can consummate E-commerce transactions while taking advantage of Vanuatu's low business income tax rates. Vanuatu-based websites—referred to as 'cybersuites' in the EBA —are rented to foreign parties so that they may engage in E-commerce without the necessity of establishment of a formal international corporation with directors, shareholders and a registered office. Cybersuite proprietors are provided assistance in the creation of the website and its maintenance.[135]

Selected Definitions

Cybersuite: an account created and kept by a business firm as a cybersuite account.[136]
Generally, a cybersuite is a "separate legal entity" unless the EBA provides otherwise.[137] A cybersuite must pay an annual fee of 40,000 Vatus to the government.[138]
A cybersuite may enter into a contract with another cybersuite.[139] A cybersuite is required to maintain an account with the National Bank of Vanuatu, to be used for all transactions it enters into.[140]
Cybersuite proprietor: a person who has entered into a cybersuite contract with a business firm.[141]
Cybersuite Contract: a contract entered into between a cybersuite proprietor and a business firm. This contract will regulate the rights and responsibilities of the business firm and the cybersuite proprietor pertaining to the cybersuite.[142] Ordinarily, cybersuite contracts: (1) explain the "voting and economic rights" of the cybersuite; (2) allow for the cybersuite proprietor or the business firm to raise capital by entering into debt or issuing equity shares; (3) detail when funds are to be conveyed to the cybersuite proprietor's account; and (4) determine whether economic or voting privileges are exclusive or not exclusive.[143]

Cybersuite Contracts and E-Commerce Contracts

Pursuant to the EBA, business firms may enter into contractual agreements with any person.[144] Notwithstanding any other law, business firms: (1) may engage in E-commerce transactions; and (2) may consummate E-commerce contracts or cybersuite contracts. Neither an E-commerce contract nor a cybersuite contract of a business firm may be declared 'voidable or unenforceable' because, at the time of contracting, one or more of the parties lacked contractual capacity.[145]

Licence May Not Be Required

A party to an E-commerce contract, or a party to a cybersuite contract, is not required to hold a business licence issued within Vanuatu.[146] Furthermore, they are not obliged to obtain authorization pursuant to any law of Vanuatu to commit acts within Vanuatu in furtherance of rights and responsibilities existing because of an E-commerce contract or a cybersuite contract.[147]

Legal Recognition of E-Commerce Contracts and Cybersuite Contracts

The mere fact of the electronic form of cybersuite contracts and E-commerce contracts is insufficient justification for denial of their legal 'effect, validity, enforceability or admissibility.'[148]

Vanuatu Law Controls

Unless the parties agree otherwise, the laws of Vanuatu are controlling with respect to an E-commerce contract or a cybersuite contract. These contracts will be assumed to have been formed in Vanuatu.[149]

Cybersuite and E-commerce Accounts

Electronic business activity must be recorded in either an E-commerce account or a cybersuite account.[150] Accounting rules mandate that each business firm carrying on electronic transactions keep a separate account of the activities.[151] The accounting records must indicate the property that has been assigned to each E-commerce or cybersuite account.[152]

Assets and Liabilities

Pursuant to the cybersuite contract in effect, a business firm must indicate all of its assets which have been assigned to the cybersuite.[153] If a business firm has an E-commerce account, all assets and liabilities that pertain to its E-commerce activity must be earmarked.[154] Notwithstanding the provisions of any other law, the assets of a cybersuite comprise a trust which is held by the business firm for the benefit of the cybersuite proprietors.[155]

The EBA has no effect on the rights of a cybersuite proprietor to: (1) receive a return on its investment in the cybersuite; or (2) have the cybersuite liquidated and the assets distributed to the cybersuite proprietors that have an ownership interest in said assets.[156]

Revenue, Expenses and Income

If a business firm earns regular income, interest income or acquires property as a result of investment in a cybersuite account or an E-commerce account, said income or property must be recorded in the respective cybersuite/E-commerce account.[157] If a business firm incurs 'expenses, fees or losses' as a result of its cybersuite or E-commerce activities, they must be recorded in the respective account.[158]

Treatment of Property

Generally, business firms have discretion to make decisions in reference to the property assigned to an E-commerce account in accordance with their best business judgment.[159]

A business firm owning a cybersuite account is in a different situation, however; they are not allowed to commingle the cybersuite account property with property held in other parts of the business, or substitute property from one part of the business firm with property once held by a cybersuite account.[160]

Cybersuite Termination

A business firm may liquidate a cybersuite if: (1) all cybersuite contracts and E-commerce contracts relating to that cybersuite have been completed; and (2) the obligations of all relevant parties—including the business firm, all parties which had contracted with the business firm, and the cybersuite proprietor—have been discharged.[161] If any property remains in the cybersuite after the rights of all other parties have been satisfied, said property belongs to the cybersuite proprietor.[162] However, no cybersuite property can be used to pay any creditor.[163]

Securities

A business firm is allowed to issue one or more classes of securities[164] pertaining to one or more cybersuites, provided this is not prohibited in the cybersuite contract.[165] At the time of their issuance, each security must be recorded in the business firm's records, with the name of the particular cybersuite identified.[166] A business firm has managerial discretion to make decisions as to the price, terms and conditions of the securities.[167]
Any proceeds received from the sale of the securities should be credited to the relevant cybersuite account.[168] A business firm is allowed to use cybersuite assets for the purpose of redemption or repurchase of securities.[169]

TONGA'S COMPUTER CRIMES ACT

The Computer Crimes Act[170] ('CCA') was enacted by the Tonga Legislative Assembly on 8 September 2003[171] and was signed into law by King Taufa'Ahau Tupou IV on 18 November 2003.[172] Its purpose is to 'combat computer crime and to provide for the collection and use of electronic evidence.'[173]

Selected Definitions

The CCA defines 'computer' very broadly, as an 'electronic, magnetic, optimal, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices...'[174] However, the following items are exempted from the definition and do not fall under the jurisdiction of the CCA: automatic typewriters, automatic typesetters, portable calculators, similar non-programmable devices, or such other devices as may be excluded by the Minister in a public notice.[175]
A 'protected computer' is a computer used in the achievement of a governmental function, or a computer used in the achievement of a private-sector function which impacts a significant number of members of the general public.[176] Specifically, such activities include: (1) the Kingdom of Tonga's national defence, national security or international relations;[177] (2) public safety efforts of law enforcement officials, and confidential information sources used by them;[178] (3) emergency services,[179] e.g., fire departments, hospitals and ambulances; (4) public utilities, including communications facilities and public transportation;[180] (5) public-key-infrastructure ('PKI');[181] and (6) banking services.[182]
'Hinder' has a specific meaning under the CCA. It refers to the carrying out of the following specified acts in furtherance of a computer crime, i.e.: (1) turning off the electricity to a computer; (2) inference with the operation of a computer via "electromagnetic interference;" (3) any action which 'corrupts' a computer; or (4) contaminating computer data by actions of 'inputting, deleting or altering.'[183]
'Seize' also has a specific meaning under the CCA relating to acts of execution of a computer crime. These acts include: (1) production and retention of computer data without authorization, even if the production or retention involves utilization of equipment at the site of the computer system; (2) without authorization, removal of computer data from a computer system, or prevention of others from retrieving it from a computer system; or (3) removal of a printout of computer data from the computer site.[184]
A 'service provider' refers to any entity, public or private, that enables its subscribers to communicate via computers. This term also refers to other entities which process or store computer data on behalf of its clients.[185]
'Traffic data' consists of computer data pertaining to a communiqué achieved via a computer system. The computer system that produces and transmits the message itself will also create and transmit the traffic data. The purpose of the traffic data is to indicate the communiqué's 'origin, destination, route, time, date, size, duration or the type of underlying services.'[186]

'Long Arm' Jurisdiction

Of course, acts carried out within the borders of the Kingdom of Tonga in furtherance of a computer crime will be in violation of the CCA. Since the internet is an international phenomenon, knowing no borders, it is also possible for persons or entities located in foreign countries to effectuate computer crimes impacting the Kingdom of Tonga. For that reason, the CCA claims 'long arm' jurisdiction over foreign individuals and entities committing acts which have an illegal impact within Tonga.[187] Those foreign-based parties will be assumed to have been within Tonga at the time the acts were committed;[188] and/or their computer, or its program or data, will be assumed to have been in Tonga at that time.[189]

Criminal Offences

Obtaining Illegal Access to a Computer

It is a crime to wilfully, without legal excuse:[190]

1. Access a computer system.[191] The maximum punishment will be a fine not exceeding $10,000, imprisonment for two years, or both;[192] and to
2. Access a 'protected' computer[193]—one used in carrying out a governmental function, or one used in carrying out a private-sector function which impacts a significant number of people.[194] Obviously, this is a more serious offence than (1), above and is deserving of a more stringent maximum punishment: a fine of $100,000, imprisonment for twenty years, or both.[195]Actual knowledge of the culprit that the computer was a 'protected' one is not required; it will be sufficient if the person either knew, or should have known, that it was a protected computer.[196]

Furthermore, for both of the above crimes, there is no need to prove that the suspect had actual knowledge that access to the computer, program or data was prohibited. Knowledge of the suspect will be presumed if there was an obvious warning presented to the accused, informing her that access to the computer, program or data was prohibited.[197]

Interference with Computer Data

It is a crime to, wilfully or recklessly, with no lawful excuse:[198]

1. damage or corrupt computer data;[199]
2. change computer data to the extent that it becomes unusable, is nonsensical or worthless;[200]
3. interfere with computer data, or meddle with others' utilization of computer data so that it is impossible to use the data in the manner desired;[201] or
4. prevent access to others who have a legal right to obtain possession of the data.[202]

The maximum punishment is a $10,000 fine, two years' imprisonment, or both.[203]

Interference With a Computer System

It is a crime, either wilfully or recklessly, with no excuse,[204] to either:

1. 'hinder' a computer system by interference with its functions;[205] or
2. 'hinder' a person who is using or operating a computer system.[206]

The maximum punishment is a $5,000 fine, an imprisonment of one year, or both.[207]

Illegal Interception of Computer Data

It is a crime to wilfully, without a legal excuse, to technically intercept[208] the following:

1. Data or a message that is being transmitted to a computer, from a computer, or within a computer;[209] or
2. A computer system's 'electromagnetic emissions' that contain computer data.[210]

For commission of either act, the maximum punishment will be a $5,000 fine, one year's imprisonment, or both.[211]

Trafficking in Illegal Computer Devices

It is a crime[212] to:

1. a. Wilfully or recklessly, without legal excuse, engage in trafficking (i.e., production, sale, procurement, importation, exportation, distribution or supplying)[213] of devices or computer programs which are intentionally created for the purpose of violation of the Computer Crimes Act, Section 4, 5, 6 or 7;[214] or
   b. Wilfully or recklessly, without legal excuse, engage in trafficking (i.e., production, sale, procurement, importation, exportation, distribution or supplying)[215] of a 'computer password, access code or similar data' which is intentionally designed to be used to facilitate the access of a computer system.[216]

2. Have in one's possession an item referenced in (1)(a) or (1)(b), above, with the intent that the item be used by any person to violate the Computer Crimes

Act, Section 4, 5, 6, or 7.[217] If more than one such item is possessed, it is presumed that she had the intent for all of the items to be used in furtherance of violation of the Computer Crimes Act, Section 4, 5, 6 or 7.[218]

The maximum punishment for both of the aforementioned offences is a fine of $20,000 and imprisonment for four years, or both.[219]

Procedural Powers

Warrants Allowing Search and Seizure by Police

If sworn evidence is presented to a judge, magistrate or other court official, and based upon said evidence, the court official is satisfied that reasonable grounds exist to suspect that a certain 'computer, computer system, computer data or data storage medium':[220]

1. may be 'material evidence' in proving an offence listed in the Computer Crimes Act; [221] or
2. is now in possession of a person due to the commission of an offence listed in the Computer Crimes Act;[222]

then said court official may issue a warrant allowing a police officer to enter the premises at which the said items are located in order to search and/or seize the said items.[223]

The police officer or other person effectuating the search and seizure must, at the time it is carried out or 'as soon as practicable,'[224] make a list of the items in question, with date and time searched/seized,[225] and give a copy of the list to the person occupying the premises[226] or the person in charge of the computer system.[227]

Ordinarily, the police officer effectuating the search and seizure should grant access to the person who had custody of the computer system for the purpose of copying computer data from the system,[228] or the police officer may make the copy and then give it to said person.[229] However, he police officer may refuse to grant access or copies of the seized material if giving the access or providing the copies would:[230]

1. violate a criminal law;[231] or
2. would prejudice an ongoing related criminal investigation, an ongoing unrelated criminal investigation, or any pending or possible criminal proceedings that may occur based upon these investigations.[232]

Assisting Police

Any person possessing or controlling an item that is the subject of a Search and Seizure under Section 9 of the Computer Crimes Act has a duty to permit the relevant police officer to do the following (and to assist her if necessary):[233]

1. Obtain access to the computer in question, or the computer data storage medium in question, to search data located in it;[234]
2. Obtain and copy said data;[235]
3. Use the said computer equipment to produce copies;[236] and
4. Produce an 'intelligible output' from the computer system in a readable format.[237]

Any person refusing, with no legal excuse, to permit a police officer to effectuate a lawfully-issued warrant, or who refuses to assist the police officer if required to do so, commits a crime. The maximum punishment will be a fine of $10,000, two years' imprisonment, or both.[238]

Production of Data

A police officer may apply to a judge, magistrate or other court official for the issuance of a court order to compel the production:[239]

1. of specific computer data, or a 'printout or other intelligible output' of said data, by the person in charge of the computer system;[240]
2. of information pertaining to subscribers by an internet service provider;[241] or
3. of a compilation of specific computer data by the person having access to the computer system, and presenting it to a specified third party.[242]

Disclosure of Information Pertaining to Traffic of Computer Data

A police officer may apply to a judge, magistrate or other court official for the issuance of a court order demanding the following information pertaining to a computer system under investigation:[243]

1. the service providers used;[244] or
2. the path travelled by some specific information under investigation.[245]

In order for the order to be issued, the court official must be satisfied that the specific data in question is 'reasonably required' in order to achieve the successful completion of a criminal investigation or proceeding.[246]

Data Retention

A police officer carrying out an investigation of an alleged computer crime may give notice in writing[247] to a person in charge of a computer system to preserve certain specified required[248] data for up to seven days,[249] provided that the police officer believes the security of the data may be in jeopardy.[250] If more time is needed by the police officer, she may apply to a judge, magistrate or other court official for an extension not to exceed fourteen days.[251]

Interception of Suspect's Communiqués by Police or Internet Service Provider

If a judge, magistrate or other court official is satisfied that 'reasonable grounds' are present indicating that the content of a suspect's communiqués and related data is necessary for the completion of a criminal investigation, the said official may issue a court order which:[252]

1. requires an internet service provider to monitor a subscriber's communiqués and to submit the collected data to the police;[253] or
2. allows the police to directly monitor communiqués of the suspect and to collect the necessary data.[254]

Interception of Traffic Data

A police officer investigating a computer crime may issue a written notice to the person in charge of a computer system.[255] The notice may request said person to: (1) make a record of the traffic of a specified type of communication during a period in question;[256] and (2) give the police the record of the data traffic after it has been compiled, or assist the police in making the record.[257] In the alternative, a court official may issue a court order permitting a police officer to gather by 'technical means' said data pertinent to a specific communiqué referenced in the order.[258]

Rules of Evidence

In cases of alleged violation of Section 6 of the Computer Crimes Act (Interference With a Computer System),[259] the mere fact that evidence presented in court has been generated by the computer system in question[260] does not automatically prevent it from being admitted.[261]

Breach of Subscriber's Confidentiality by Internet Service Provider

It is a crime for an Internet Service Provider to disclose, without legal excuse,[262] confidential information of the subscriber pertaining to: (1) the fact that a court order has been issued as part of a criminal investigation of the subscriber, pursuant to Criminal Crimes Act ss. 11, 12, 13, 14 or 15;[263] (2) any specific acts carried out pursuant to said court order;[264] or (3) any data gathered pursuant to the said court order.[265]

The maximum punishment for this crime is a $50,000 fine, ten years' imprisonment, or both.[266]

Notwithstanding the above, it is not a crime for an Internet Service Provider to disclose information as required pursuant to ss 11-15 of the Computer Crimes Act.[267]

Implementation Regulations to be Adopted

If the Cabinet gives permission, the Minister responsible for telecommunications will be responsible for the drafting of implementation regulations in order to achieve full execution of the Computer Crimes Act.[268]

SUMMARY AND RECOMMENDATIONS

Vanuatu

Summary

The Republic of Vanuatu's Electronic Transactions Act ('ETA') is designed to stimulate E-commerce in the country by improving the integrity and security of electronic transactions. The ETA recognizes the legal validity of electronic documents and electronic signatures as acceptable substitutes for paper documents and ink signatures, respectively; accordingly, electronic records may be used to comply with a statutory writing requirement, delivery requirement, original document requirement and retention requirement, and an electronic signature attached to an electronic document may be used to comply with a statutory requirement for a paper-and-ink signature. If all parties are in agreement, an E-commerce contract may be in electronic form. If a sender of an electronic message demands an acknowledgement of receipt, the message is not considered to have been received until the sender obtains the acknowledgement. Specific rules pertaining to attribution of electronic messages, and time/place of sending/receiving electronic messages, have been developed.

In order to achieve more reliability and integrity in the utilization of electronic signatures in E-commerce, the ETA has created a compulsory system of licensing of Certification Authorities ('CA'). The CA's role is to ascertain the identity of its subscribers and to attest that the electronic signature used by those subscribers belongs to them. An unusual characteristic of Vanuatu law is that a subscriber is allowed to use a pseudonym so long as the CA knows the real identity of the subscriber and keeps that information on file. The prospective CA must possess a high degree of expertise in reference to electronic signatures and computer information systems. If at any time the government believes that a CA is no longer qualified to carry out its duties, the government may suspend or revoke the CA's license. Because E-commerce is an international phenomenon, the ETA provides for reciprocal recognition of CA's with licenses issued by foreign nations that have licensing standards that are at least as stringent as those of Vanuatu. The CA may incur legal liability to its subscribers and to relying third parties if any information contained in the certificate is inaccurate, if the subscriber does not hold the private key on the date of issuance of the certificate, or if the private key and the public key do not have a functional interactive relationship. However, the CA's liability may be limited if the relying third party knew of the inaccuracies in the certificate, the subscriber provided false information and the CA showed due diligence, or the CA has listed limitations on liability in the certificate.

As a general rule, intermediaries such as internet service providers are not liable for the content of the electronic messages which they disseminate. Notwithstanding this general rule, intermediaries may incur liability for defamation if they have knowledge that certain material is defamatory. If an intermediary suspects that material is defamatory but does not have knowledge, then the intermediary should inform the Minister in charge of telecommunications and await her determination on the matter before dissemination of the material.

Vanuatu's E-Business Act ('EBA') is a remarkable statute because it allows foreign individuals and entities to rent a website in Vanuatu and to use that website to carry out international E-commerce activity, without having to establish a formal international corporation with directors, shareholders and a registered office. The EBA creates an 'Internet Free Trade Zone' in which website-renters are able to take advantage of Vanuatu's low business income tax rates. Renters are even provided assistance in the creation of their websites.

Recommendations

Vanuatu's statutes are a good beginning in promotion of E-commerce; they do not go far enough, however. These additions need to be made: (1) consumer protections need to be included in order to give more notice to cyber-buyers, to give them a brief window of opportunity to back out of an online purchase, and to give them more security against the possibility of cyber-fraud; (2) a detailed list of computer crimes needs to be added in order to inhibit hackers from commission of privacy violations and to protect against computer tampering (refer to the Tonga portion of this article for an example of a computer crimes statute); and (3) mandatory requirements for governmental agencies to begin to allow citizens to utilize electronic documents and signatures should increase governmental efficiency, cut costs and allow taxes to continue to be kept at a low level.

Tonga

Summary

If Vanuatu is in need of a computer crimes law, it can refer to the Kingdom of Tonga's Computer Crimes Act ('CCA'). The CCA allows 'long arm' jurisdiction. Under the CCA, the following activities are defined to be crimes and offenders may incur fines and/or imprisonment: obtaining illegal access to a computer; interfering with another's computer system; unlawfully intercepting computer data; and trafficking in illegal computer devices. To enforce the CCA, the police may be granted warrants authorizing them to search a suspect's premises, to seize a suspect's computer system or contraband items, to intercept a

suspect's electronic communiqués, or to require a suspect to retain specific computer data for a given amount of time. Any party suspected of violation of the CCA must cooperate fully with the police and produce any computer data that is requested. Internet service providers may also be compelled to allow the police to have access to any computer-borne information pertaining to a subscriber that is suspected of violation of the CCA.

Recommendations

Just as Vanuatu can learn from Tonga, Tonga can also learn from Vanuatu. Tonga needs to enact: (1) a comprehensive electronic transactions statute comparable to Vanuatu's ETA in order to stimulate the growth of E-commerce by improving the reliability and integrity of E-commerce transactions; and (2) a statute comparable to Vanuatu's EBA in order to foster the development of Tonga as a tax haven for foreign entities seeking to carry out international E-commerce transactions. These statutes could be easily implemented and might result in the government's reaping of substantial cash inflows with little or no detrimental effects. Given the Tongan government's current financial crisis, such new means of increasing the flow of funds into its coffers should be experimented with.

---

[1] PhD Candidate (Law), The University of Hong Kong; PhD (Business Administration), University of Arkansas, 1979; JD *cum laude*, Texas Southern University, 1986; LLM (Int'l Bus. Law) University of Houston, 1992; LLM (Info. Tech. Law) *with distinction*, University of Strathclyde (Scotland), 2005. Attorney at Law, Texas and Oklahoma; C.P.A., Texas. He practiced solo (employment-discrimination litigation) in Houston, Texas, was affiliated with the Cheek Law Firm (insurance-defence litigation) in Oklahoma City, and has engaged in management consulting in China. Additionally, he has taught law, accounting, and management at twelve universities located in the U.S.A., Africa and the Middle East.

[2] Although decades have passed since Vanuatu achieved its independence, some still contend that the nation remains overly dependent on aid from foreign countries and that economic independence has not been attained. Furthermore, Vanuatu has too many rich, influential white persons controlling the business sector, and too few natives that have been able to pull themselves out of poverty and assume business management positions. According to a former New Zealand High Commissioner to Vanuatu, Brian Smythe, this situation is bound to build resentment among the natives of Vanuatu "and that resentment could lead to trouble." See Ricky Binihi, 'Vanuatu Economy—An Expatriate Enclave, Says Smythe,' *Port Vila Presse* (Port Vila, Vanuatu), 8 February 2005, 1, at http://www.news.vu/en/news/national/050207-vanuatu-economy-an-expatriate-enclave.shtml (Accessed 06 July 2006).

[3] U.S. Central Intelligence Agency ('CIA'), 'Vanuatu,' *The World Factbook* 1-2 (1 November 2005), at http://www.cia.gov/cia/publications/factbook/print/nh.html (Accessed 06 July 2006).

[4] Australian Department of Foreign Affairs and Trade, *Vanuatu Country Brief—November 2005* 1; http://www.dfat.gov.au/geo/vanuatu/vanuatu_brief.html (Accessed 06 July 2006).

[5] U.S. Department of State, Bureau of East Asian and Pacific Affairs, *Background Note—Vanuatu* (October, 2005) 1, at http://www.state.gov/p/eap/ci/nh/ (Accessed 06 July 2006).

[6] 'Vanuatu—Economy,' *Geography IQ* (2006), at

http://www.geographyiq.com/countries/nh/Vanuatu_economy_summary.htm (Accessed 06 July 2006).

[7] In response to complaints from the governments of several foreign countries, the government of Vanuatu has pledged to increase legal controls over its financial institutions which serve foreign individuals and foreign firms. 'Vanuatu's Economy,' *Travelblog: Free Inspiration* (January, 2006) 1; available at http://www.travelblog.org/World/nh-econ.html (Accessed 06 July 2006). Furthermore, the government of Vanuatu has intermittently been criticised for increasing taxes. *See* Evelyn Toa, 'Where is Vanuatu's Economy Going?,' *Port Vila Presse* (Port Vila, Vanuatu) 26 June 2003, 1, at http://www.news.vu/en/business/Economy/142.shtml (Accessed 06 July 2006).

[8] U.S. Department of State, Note 3 above at 3.

[9] Note 4 above.

[10] CIA, Note 2 above at 5-6. The tourism industry of Vanuatu now employs an estimated 1,200 people. Australian Department of Foreign Affairs and Trade, Note 4 above at 2. After Pacific Blue began to offer airline service to Vanuatu in September 2004, the number of tourists increased by 20% within six months. Additionally, construction of new hotels and resorts is underway. Id. at 3. For a listing of websites relating to Vanuatu tourism, see Government of the Republic of Vanuatu, *Directory of Internet Sites Related to Vanuatu* 5-6, at http://www.vanuatugovernment.gov.vu/directory.html (Accessed 06 July 2006).

[11] Australian Department of Foreign Affairs and Trade, Note 4 above at 2.

[12] U.S. Department of State, Bureau of East Asian and Pacific Affairs, *Background Note: Tonga* (December, 2005) 2, at http://state.gov/r/pa/ei/bgn/16092.htm (Accessed 06 July 2006).

[13] Tonga Visitors Bureau, 'Tonga's Economy,' *The Kingdom of Tonga: Ancient Polynesia* 1, at http://www.tongaholiday.com/experience/about/economy.php (Accessed 06 July 2006).

[14] CIA, 'Tonga,' *The World Factbook* (1 November 2005), 1-2, at http://www.cia.gov/cia/publications/factbook/print.tn.html (Accessed 06 July 2006).

[15] 'Tonga,' *Wikipedia* (2005), at http://en.wikipedia.org/wiki/Tonga (Accessed 06 July 2006).

[16] U.S. Department of State, Note 12 above at 1-2.

[17] David Fickling, 'From Squash to Space Tourism,' *Guardian Unlimited* 4 November 2002, 2, at http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,829914,00.html (Accessed 06 July 2006).

[18] European Union, *Tonga: Country Overview* (2006) 1, at http://europa.eu.int/comm/development/body/country/country_home_en.cfm?cid=to&lng=en&status=new#overview (Accessed 06 July 2006).

[19] *Wikipedia*, Note 15 above.

[20] European Union, Note 18 above at 2.

[21] David Fickling, Note 17 above at 2-3. Examples include a plan to use Tonga as a launching pad for a space tourism firm, a plan to use Tonga as a refining point for Iranian crude oil, and a 'bogus scheme to turn seawater into natural gas.' Id.

[22] Id. at 2.

[23] 'Tonga: Economy Hits Rock Bottom, Commerce Minister Says,' *Pacific Islands: Pina and Pacific* (11 January 2006), at http://www.pacificislands.cc/pina/pinadefault2.php?urlpinaid=19482 (Accessed 06 July 2006).

[24] Mary Fonua, 'Grim Outlook for Tongan Economy in Wake of Strike Settlement,' *Matangi Tonga* (11 December 2005) 1-4, at http://www.matangitonga.to/article/tonganews/economy/grimoutlook111205.shtml ((Accessed 06 July 2006)). Government health services are especially important for the 18% of adult Tongans that are diabetics. Id. at 4.

[25] *Utah Code Annotated* 46-3-101 et seq. (1999).

[26] Jochen Zaremba, 'International Electronic Transaction Contracts Between US and EU Companies and Customers,' (2003) 18 *Connecticut Journal of International Law* 479, 511. Vanuatu law defines an electronic signature as 'a signature in electronic form in, attached to, or logically associated with, information that is used by a signatory to indicate his or her adoption of the content of that information...'

ETA, Note 42 below s 1. This is an inclusive definition and is evidence of technological open-mindedness.

[27] Jochen Zaremba, Id.

[28] Under Vanuatu law, a digital signature complies with the requirements contained in the definition of an Electronic Signature: it must be unique to the signatory, identify the signatory, be created by a means under the signatory's sole control, and be linked to a data message so that any alterations to the data message since its creation can be determined. ETA, s 1.

[29] Note 25 above.

[30] It is debatable as to whether technological-neutrality or technological-specificity is the correct road to take. *See* Sarah E. Roland, Note, 'The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?' (2001) 35 *Suffolk University Law Review* 625, 638-45

[31] For concise coverage of the United Nations, European Union, British and American law of digital signatures, *see* Stephen E. Blythe, 'Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security,' (2005) 11:2 *Richmond Journal of Law and Technology* 6.

[32] In terms of relative degree of technological neutrality, Vanuatu seems to have adopted the 'hybrid' model—a preference for the digital signature, but not to the exclusion of other forms of electronic signatures.

[33] Richard Wu, 'Electronic Transaction Ordinance—Building a Legal Framework for E-commerce in Hong Kong,' (2000) 2000:1 *Journal of Information Law and Technology* 5-9, at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_1/wu/ (Accessed 06 July 2006).

[34] Renard Francois, Comment, 'Fair Warning, Pre-emption and Navigating the Bermuda Triangle of E-Sign, UETA, and State Digital Signature Laws,' (2001) 19 *John Marshall Journal of Computer and Information Law* 401, 405-06.

[35] American Bar Association ('ABA'), *PKI Assessment Guidelines*, V 0.30 at 301 (Public Draft for Comment No. 25, 2001), at http://www.abanet.org/scitech/ec/isc/pagv30.pdf (Accessed 06 July 2006).

[36] ABA, *PKI Assessment Guidelines*, Id. at 305.

[37] American Bar Association, Section of Science & Technology, Information Security Committee, Electronic Commerce & Information Technology Division, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (1995 and 1996) 9; http://www.abanet.org/ftp/pub/scitech/ds-ms.doc (Accessed 06 July 2006).

[38] Aristotle Mirzaian, Esq., 'Electronic Commerce: This is Not Your Father's Oldsmobile,' (2002) 26 *Rutgers Law Record* 7, 13.

[39] Vanuatu law provides that Certification Authorities are responsible for the issuance of 'identity certificates for the purposes of electronic signatures or provides other services to the public related to electronic signatures.' ETA, Note 42 below, s 1.

[40] Michael H. Dessent, 'Digital Handshakes in Cyberspace Under E-Sign: 'There's A New Sheriff in Town!' (2002) 35 *University of Richmond Law Review* 943, 992.

[41] Jane Kaufman Winn, 'The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce,' (2001) 37 *Idaho Law Review* 358, 384-88.

[42] *Electronic Transactions Act* (Act. 24 of 2000) (Republic of Vanuatu) (hereinafter 'ETA'), at http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/eta2000256.html (Accessed 06 July 2006). For a discussion of the ETA by the Prime Minister of Vanuatu—the person who introduced the bill in Parliament—see Hon. Prime Minister Barak T. Sope Maautamate, MP, Government of the Republic of Vanuatu, *The E-Business Act of 2000, The International Companies (E-Commerce Amendment) Act of 2000, The Companies (E-Commerce Amendment) Act of 2000: A Plain English Explanation*, pp. 3-7, at http://www.vanuatu.gov.vu/government/library/Exp%20note%20ecommerce%20acts.doc (Accessed 06 July 2006).

[43] Id. at Preamble.

[44] Id. at Preamble.

[45] In order to promote security of E-commerce transactions, business firms renting 'cybersuite' websites in Vanuatu pursuant to the E-Business Act are also required to comply with the ETA. EBA, Note 131 below, s 15(1). More specifically, each firm must appoint a 'data protection officer' to coordinate the implementation of the information security procedures. EBA, Note 131 below, s 15(2).

[46] ETA s 2.

[47] ETA s 3. For a paper relating to the inability of the common law of contracts to adequately deal with E-commerce transactions, and the need for Vanuatu to enact specific legislation in emulation of the UNCITRAL Model Law (covered in the article referenced in footnote 31 above), *see* Philip Tagini, 'E-commerce in Vanuatu: Can Contract Law Accommodate For New Technology?,' (2000) 4 *Journal of South Pacific Law*, Working Paper 2, 10.

[48] 'Vanuatu E-commerce,' *Lowtax* 1, at http://www.lowtax.net/lowtax/html/jvaecom.html (Accessed 06 July 2006).

[49] ETA s 4. This includes the generation, sending, receiving, storing and processing of electronic records. Id.

[50] ETA s 1. The telecommunications Minister is responsible for enforcement of the ETA. Id.

[51] ETA s 5.

[52] The emerging trend is for this exception to be eliminated. In 2005, the U.S. State of Tennessee became the first American jurisdiction to recognize the legal validity of a will that is executed with an electronic signature. *See* Chad Michael Ross, Comment, 'Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will,' (2005) 35 *University of Memphis Law Review* 603.

[53] ETA s 6.

[54] ETA s 7.

[55] Id. at s 1. The other twenty-two terms are: addressee, appropriate law enforcement agency, approved form, certification service provider, data controller, data processor, E-commerce service provider, electronic agent device, electronic record, electronic signature (covered in footnote 26 above), electronic signature product, identifiable individual, information, information processing system, intermediary, Minister, originator, personal data, prescribed, record, signature creation device, and signature verification device. Id.

[56] An 'accredited certificate' is often simply referred to as a 'Certificate' in other jurisdictions, and that is the term that will be used in this article.

[57] This position is often referred to as the 'Certification Authority' ('CA') in other jurisdictions, and that is the phrase which will be used in this article.

[58] ETA s 8.

[59] ETA s 9(1). This is applicable regardless of whether the information is affirmatively mandated to be in writing, or consequences will be applied to the situation if there is no writing. ETA s (2).

[60] ETA s 10(1).

[61] ETA s 10(2).

[62] ETA s 11(1).

[63] ETA s 11(3).

[64] ETA s 19.

[65] If there is 'reliability,' the information will suit the purpose for which it was created and all of circumstances of the particular situation. ETA s 12(3).

[66] If there is 'integrity,' the information will be exactly the same as in the original, except for endorsement or changes occurring due to 'communication, storage and display.' ETA s 12(3).

[67] ETA s 12(1).
[68] ETA s 12(2).
[69] ETA s 13(1). If there is an obligation to store an electronic document, that obligation does not attach to any information used only for the transmission or reception of an electronic message. ETA s 13(2). Furthermore, satisfaction of the retention requirement using electronic records can be achieved via the services of another person. ETA s 13(3).
[70] ETA s 14(1).
[71] ETA s 14(2).
[72] ETA s 15(1).
[73] ETA s 15(2).
[74] ETA s 16(1).
[75] ETA s 16(2).
[76] ETA s 17(1). However, this section does not concern itself with the 'legal consequences' of the electronic message or from the receiver's acknowledgement of receipt. ETA s 17(6).
[77] ETA s 17(2).
[78] ETA s 17(3).
[79] ETA s 17(4).
[80] ETA s 17(5).
[81] ETA s 18(1).
[82] ETA s 18(2). These rules apply regardless of whether the computer system's location is different than the assumed place of dispatch/reception as determined in ETA s 18(4). ETA s 18(3).
[83] ETA s 18(4). If either the sender or the receiver has more than one place of business, then the assumed point of transmission/reception is the one having the closest association with the transaction in question. If there is not a close association present, then the principal place of business is the applicable location. ETA s 18(5)(a). If the party has no place of business, the point of transmission/reception is the residence of the party. ETA s 18(5)(b).
[84] ETA s 19.
[85] ETA s 20(1).
[86] ETA s 20(2).
[87] ETA s 20(3). These requirements appear to be too nebulous and not rigorous enough. The requirements for issuance of a CA's licence are much more stringent and specific in some other jurisdictions, e.g., Hong Kong and Korea. *See* Stephen E. Blythe, 'Hong Kong Electronic Signature Law and Certification Authority Regulations: Promoting E-Commerce in the World's Most Wired City,' (2005) 7:1 *North Carolina Journal of Law and Technology* 1; and Stephen E. Blythe, 'The Tiger on the Peninsula is Digitized: Korean E-Commerce Law as a Driving Force in the World's Most Computer-Savvy Nation,' (2006) 28:3 *Houston Journal of International Law* __ . However, it should be kept in mind that Vanuatu is a developing country and that its typical E-commerce transaction may be of a lower financial amount that in Hong Kong or Korea; hence, it may not be so necessary for a Vanuatu CA to have substantial capital.
[88] ETA s 20(3).
[89] ETA s 20(4).
[90] ETA s 20(5).
[91] ETA s 20(6).
[92] ETA ss 20(4) and (7).
[93] ETA s 21(1).
[94] ETA s 21(2).
[95] ETA s 21(3).

[96] ETA ss 20(4)--(7).
[97] ETA s 22(1). This is the first instance the author has seen anywhere allowing an assumed name to appear on the Certificate. Of course, the subscriber must present sufficient identification to enable the CA to confirm the subscriber's real identity.
[98] ETA s 22(2).
[99] ETA s 22(3).
[100] ETA s 23(1)(a)--(c).
[101] ETA s 23(1).
[102] The CA must have taken "all reasonably practical measures" in its verification efforts. ETA s 23(2)(b).
[103] ETA s 23(2)(a) and (b).
[104] ETA s 23(4).
[105] ETA s 23(3).
[106] ETA s 24(2).
[107] ETA s 24(1).
[108] ETA s 25(1).
[109] ETA s 25(2).
[110] ETA s 25(3)
[111] One million Vatus is approximately U.S. $ 9,285.
[112] ETA s 25(4).
[113] E.g., an internet service provider.
[114] ETA s 26(1).
[115] ETA s 26(2).
[116] ETA s 26(3).
[117] ETA s 27(1)(a).
[118] ETA s 27(1)(b).
[119] ETA s 27(2).
[120] ETA s 27(3).
[121] ETA s 27(4).
[122] ETA s 28(1).
[123] ETA s 28(2).
[124] ETA s 28(3).
[125] ETA s 28(4).
[126] ETA s 29(1).
[127] ETA s 29(2).
[128] ETA s 29(3). One hundred thousand Vatus is approx. U.S. $929.
[129] ETA s 30(1).
[130] ETA s 30(2). Fifty thousand Vatus is approx. U.S. $464.
[131] *E-Business Act* (Act No. 25 of 2000) (Republic of Vanuatu) (hereinafter 'EBA'), at http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/ea2000125.html (Accessed 06 July 2006). For a discussion of the E-Business Act by the Prime Minister of Vanuatu—the person who introduced the bill in Parliament. See Note 42 above at 8-10.
[132] EBA at Preamble.
[133] The Minister may promulgate regulations necessary for the effective implementation of the EBA. EBA s 19.

[134] EBA at Preamble. Two other statutes, not covered in this article, have an impact on E-commerce law in Vanuatu. The International Companies Act, covering foreign firms, now includes E-commerce activities in its scope; *see International Companies (E-Commerce Amendment) Act* (Act No. 26 of 2000) (Republic of Vanuatu), at http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/icaa2000397.html (Accessed 06 July 2006). Additionally, The Companies Act, covering domestic firms, now includes E-commerce activities in its scope; *see Companies (E-Commerce Amendment) Act* (Act No. 27 of 2000) (Republic of Vanuatu), at http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/caa2000258/caa2 (Accessed 06 July 2006).

[135] *Lowtax*, Note 48 above.

[136] EBA s 2(1).

[137] EBA s 2(2).

[138] EBA s 17(1). Forty thousand Vatus is approximately U.S. $371. The fee is payable 'on or before 30 June' of each year. Id. If it is not paid in a timely manner, a penalty will be assessed for late payment. EBA s 17(2). The fee (and the penalty, if applicable) is a debt due and owing to the government and may be recovered by the government in a court action. EBA s 17(3).

[139] EBA s 2(3).

[140] EBA s 18(1). If this requirement is not complied with, the cybersuite has committed a crime and it may be fined an amount not to exceed 5 million Vatus (approx. U.S. $46,425). EBA s 18(2).

[141] EBA s 1.

[142] EBA s 3(1).

[143] EBA s 3(2).

[144] EBA s 4(1).

[145] EBA s 4(2).

[146] EBA s 5(1)(a).

[147] EBA s 5(1)(b). However, this provision is inapplicable to cybersuite proprietors, or parties who have entered into cybersuite contracts or E-commerce contracts, if they are: (1) a 'local company' according to the Vanuatu Companies Act; or (2) a Vanuatu resident; or (3) licensed to engage in certain business activities pursuant to the Vanuatu Companies Act, Schedule 3; or (4) they are foreign, but allowed to engage in business within Vanuatu with a Vanuatu person or entity pursuant to the Vanuatu Companies Act, s 378(1)(c)(iii). EBA s 5(2).

[148] EBA s 6.

[149] EBA s 7.

[150] EBA s 8.

[151] EBA s 9(1).

[152] EBA s 9(2).

[153] EBA s 10(1). A value must be assigned to all such assets and liabilities. EBA s 10(3).

[154] EBA s 10(2). A value must be assigned to all such assets and liabilities. EBA s 10(3).

[155] EBA s 10(4).

[156] EBA s 10(5).

[157] EBA s 11(1).

[158] EBA s 11(2). A business firm incurring expenses, fees or losses may subtract this amount from the account in question. This deduction will have the effect of making that portion no longer a part of the assets assigned to that cybersuite or E-commerce account. EBA s 11(3).

[159] EBA s 12(1).

[160] EBA s 12(2).

[161] EBA s 13(1).

[162] EBA s 13(2).
[163] It makes no difference if the creditor is secured or unsecured; the prohibition still applies. EBA s 16(2).
If any other law states the contrary, this provision is nevertheless controlling. EBA s 16(1).
[164] Securities are stocks (equity) and bonds (debt).
[165] EBA s 14(1).
[166] EBA s 14(2).
[167] EBA s 14(3).
[168] Id. Fees, taxes and other expenses incurred as a result of the sale should be deducted from the proceeds, and recorded in the cybersuite account. Id.
[169] EBA s 14(4). This is generally allowed, notwithstanding the prohibition of this type of action in the *Vanuatu International Companies Act*, parts 4 and 9. Id. However, redemption or repurchase using cybersuite property is not allowed if this is in contravention of the 'terms and conditions on which the securities were issued.' Id.
[170] *Computer Crimes Act* (Act. No. 14 of 2003) (Kingdom of Tonga) (hereinafter 'CCA'), at http://www.paclii.org/to/legis/num_act/cca2003185/ (Accessed 06 July 2006).
[171] Id. at Preamble.
[172] Id. at Preamble and s 18.
[173] Id. at Preamble.
[174] Id. at s 2.
[175] Id.
[176] Id. at s 4(1).
[177] Id. at s 4(1)(a).
[178] Id. at s 4(1)(b) and (d).
[179] Id. at s 4(1)(d).
[180] Id. at s 4(1)(c).
[181] Id.
[182] Id.
[183] Id. at s. 2.
[184] Id.
[185] Id.
[186] Id. at s 2.
[187] Id. at s 3(1)
[188] Id. at s 3(2)(a).
[189] Id. at s 3(2)(b).
[190] Id. at ss 4(2) and 4(3).
[191] Id. at s 4(2).
[192] Id. In this article, the amounts of all CCA fines are expressed in U.S. Dollars. The currency of Tonga is the Pa'anga. As of 30 January 2006, One U.S. Dollar is approx. 2.06 Tonga Pa'angas. Source: XE.com.
[193] CCA at s 4(1).
[194] Id. at s 4(1)(a)-(d).
[195] Id. at s 4(3).
[196] Id. at s 4(1).
[197] Id. at s 4(4).
[198] Id. at s 5.

[199] Id. at s 5(a).
[200] Id. at s 5(b).
[201] Id. at s 5(c) and (d).
[202] Id. at s 5(e).
[203] Id. at s 5.
[204] Id. at s 6.
[205] Id. at s 6(a).
[206] Id. at s 6(b).
[207] Id. at s 6.
[208] Id. at s 7.
[209] Id. at s 7(a).
[210] Id. at s 7(b).
[211] Id. at s 7.
[212] Id. at s 8(1).
[213] Id. at s 8(1)(a).
[214] Id. at s 8(1)(a)(i).
[215] Id. at s 8(1)(b).
[216] Id. at s 8(1)(a)(ii).
[217] Id. at s 8(1)(b).
[218] Id. at s 8(2).
[219] Id. at s 8(1).
[220] Id. at s 9(1).
[221] Id. at s 9(1)(a).
[222] Id. at s 9(1)(b).
[223] Id. at 9(1).
[224] Id. at s 9(2).
[225] Id. at s 9(2)(a).
[226] Id. at s 9(2)(b)(i).
[227] Id. at s 9(2)(b)(ii).
[228] Id. at s 9(3)(a).
[229] Id. at s 9(3)(b).
[230] Id. at s 9(4).
[231] Id. at s 9(4)(a).
[232] Id. at s 9(4)(b).
[233] Id. at s 10(1).
[234] Id. at s 10(1)(a).
[235] Id. at s 10(1)(b).
[236] Id. at s 10(1)(c).
[237] Id. at s 10(1)(d).
[238] Id. at s 10(2).
[239] Id. at s 11.
[240] Id. at s 11(a).
[241] Id. at s 11(b).
[242] Id. at s 11(c).

[243] Id. at s 12.
[244] Id. at s 12(a).
[245] Id. at s 12(b).
[246] Id. at s 12.
[247] Id. at s 13(1).
[248] Id. at s 13(1)(a).
[249] Id. at s 13(1).
[250] Id. at s 13(1)(b).
[251] Id. at s 13(2).
[252] Id. at s 14.
[253] Id. at s 14(a).
[254] Id. at s 14(b).
[255] Id. at s 15(1).
[256] Id. at s 15(1)(a).
[257] Id. at s 15(1)(b).
[258] Id. at s 15(2).
[259] Id. at s 16(a).
[260] Id. at s 16(b).
[261] Id. at s 16.
[262] Id. at s 17(1).
[263] Id. at s 17(1)(a).
[264] Id. at s 17(1)(b).
[265] Id. at s 17(1)(c).
[266] Id. at s 17(1).
[267] Id. at s 17(2).
[268] Id. at s 18.