The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control

Stephen E. Blythe
New York Institute of Technology

Uganda drafted three proposed computer laws in 2004 which remain under consideration: The Electronic Signature Bill ("ESB") would provide for legal recognition of electronic signatures ("E-signatures"). Although all types of E-signatures are recognized, the digital signature enjoys most-favored status because it utilizes cryptographic methods. All Certification Authorities ("CA") are required to hold a license issued by the Controller of CA's and their computer system must be trustworthy. The Electronic Transactions Bill ("ETB") would provide a legal foundation for E-commerce transactions. The electronic form may be used to satisfy a statutory requirement for: a writing; a handwritten signature; an original document; retention of a paper document; and a notarized paper document. The Computer Misuse Bill ("CMB") would prohibit several types of computer crimes: unauthorized access; modification of contents; unauthorized use or interception of computer service; unauthorized obstruction of use of computer; unauthorized disclosure of access code; breach of confidentiality obligation; enhanced punishment pertinent to national security, using a computer to disseminate child pornography; and attempts and abetments. The objectives of this article are to: (1) explain the roles of electronic signatures, cryptology, public key infrastructure, and certification authorities; (2) cover the three generations of electronic signature law; (3) analyze Uganda's proposed computer laws: Electronic Signature Bill ("ESB"), Electronic Transactions Bill ("ETB"), and Computer Misuse Bill ("CMB"); and (4) make recommendations for improvement of those bills.

ELECTRONIC SIGNATURES

Contract law worldwide has traditionally required the parties to affix their signatures to a document (U.S.A., 1998). With the onset of the electronic age, the electronic signature made its appearance. It has been 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," (Smedinghoff, 1999, p.162) or as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" (E.U., 2000, p. 12). An electronic signature may take a number of forms: a digital signature, a digitized fingerprint, a retinal scan, a pin number, a digitized image of a handwritten signature that is attached to an electronic message, or merely a name typed at the end of an e-mail message (Tang, 1999).

A well-known U.S. consumer group has stated, "Given the current state of authentication technology, it's much easier to forge or steal an e-signature than a written one" (Dessent, 2002, p. 4). This statement seems to assume that all E-signatures offer an equal degree of security. However, such an assumption would be erroneous; some electronic signatures offer more security than others. It is prudent for E-commerce participants to use the more secure types of electronic signatures, notwithstanding their greater degree of complexity and expense.

Online Contracts: Four Levels of Security

When entering into a contract online, four degrees of security are possible.

A. The first level would exist if a party accepted an offer by merely clicking an "I Agree" button on a computer screen (Stern, 2002).

B. The second level of security would be incurred if secrets were shared between the two contracting parties. This would be exemplified by the use of a password or a credit card number to verify a customer's intention that goods or services were to be purchased (Stern, 2002).

C. The third level is achieved with biometrics. Biometric methods involve a unique physical attribute of the contracting party, and these are inherently difficult to replicate by a would-be cyber-thief. Examples include: a voice pattern, face recognition, a scan of the retina or the iris within one's eyeball, a digital reproduction of a fingerprint (Chung, 2003) or a digitized image of a handwritten signature that is attached to an electronic message. In all of these examples, a sample would be taken from the person in advance and stored for later comparison with a person purporting to have the same identity. For example, if a person's handwriting was being used as the biometric identifier, the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing would be recorded, and this information is almost impossible to duplicate by an imposter (Stern, 2002). Biometric identifiers have at least two drawbacks in comparison with the digital -signature: (1) The attachment of a person's biological traits to a document does not ensure that the document has not been altered, i.e., it "does not freeze the contents of the document;" and (2) The recipient of the document must have a database of biological traits of all signatories dealt with in order to verify that a particular person sent the document (Pun, 2002). The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers. Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card (Chung, 2003).

D. The digital signature is considered the fourth level because it is more complex than biometrics. Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case, however; the digital signature refers to the entire document (Hong Kong, 2000). It is "the sequence of bits that is created by running an electronic message through a one-way hash function and then encrypting the resulting message digest with the sender's private key" (Pun, 2002). A digital signature has two major advantages over other forms of electronic signatures: (1) it verifies authenticity that the communication came from a designated sender; and (2) it verifies the integrity of the content of the message, giving the recipient assurance that the message was not altered (Poggi, 2000).

Digital Signature Technology: Public Key Infrastructure

The technology used with digital signatures is known as Public Key Infrastructure, or "PKI" (Fischer, 2001). PKI consists of four steps:

A. The first step in utilizing this technology is to create a public-private key pair; the private key will be kept in confidence by the sender, but the public key will be available online (A.B.A., 2001).

B. The second step is for the sender to digitally "sign" the message by creating a unique digest of the message and encrypting it. A "hash value" is created by applying a "hash function"—a standard mathematical function—to the contents of the electronic document. The hash value, ordinarily consisting of a sequence of 160 bits, is a digest of the document's contents. Whereupon, the hash function is encrypted, or scrambled, by the signatory using his private key. Asymmetric encryption provides one of the highest—if not *the* highest—degrees of security in electronic transactions. The encrypted hash function is the "digital signature" for the document (Pun, 2002).

C. The third step is to attach the digital signature to the message and to send both to the recipient.

D. The fourth step is for the recipient to decrypt the digital signature by using the sender's public key. If decryption is possible the recipient knows the message is authentic, i.e., that it came from the purported sender. Finally, the recipient will create a second message digest of the communication and compare it to the decrypted message digest (A.B.A., 1995-96). If they match, the recipient knows the message has not been altered (Zaremba, 2003).

Advantages of the Digital Signature

Unlike biometric and other forms of electronic signatures, the digital signature will "freeze" the contents of the document at the time of its creation. Any alterations to the document's contents will result in a different hash value. Furthermore, the encryption of the hash value with the signatory's private key "links uniquely the digital signature to the signatory, i.e., the owner of the private key." Although a handwritten signature is only "signatory-specific," the digital signature is both "signatory-specific" and "document-specific" (Pun, 2002).

The digital signature is the only form of electronic signature which satisfies all three of the United Nations' security evaluation factors, i.e., that an electronic signature should: (1) authorize; (2) approve; and (3) protect against fraud. Authorization is achieved because the digital signature will accompany the document, which allows for confirmation of the identity of the signatory. Approval is attained via computation of the hash value of the electronic document, which freezes the contents of the document at the time of its creation, and allows for detection of any subsequent alterations. Finally, there is protection against fraud because it is extremely unlikely—virtually impossible—for anyone to determine a signatory's private key with only the public key as a starting point (Pun, 2002).

Disadvantages of the Digital Signature

The digital signature has at least two drawbacks. Firstly, since the private key of each person is rather difficult to memorize, they are most often stored in computers. If the computer is not kept in a secure location, the contents of the private key may be vulnerable. This heightens the necessity of maintaining the security of the private key and protecting it from intruders. However, it should be noted that this weakness of the digital signature is also common to most other forms of electronic signatures. The password or the PIN face similar security problems. Therefore, with good security policies and procedures, this disadvantage can be minimized (Pun, 2002).

The other disadvantage of the digital signature pertains to the certificate, which must be issued by a Certification Authority ("CA"). Obtaining the certificate and having to interact with the CA is somewhat inconvenient and costly for the user, but over time this disadvantage should be alleviated as digital signatures become more popular, easier to use, and cheaper (Pun, 2002). Because the CA plays such a vital role in the viability of the digital signature, it is essential for the user to understand exactly what the CA does.

The Critical Role of the Certification Authority

In order for PKI to realize its potential, it is crucial that the user be able to ensure the authenticity of the public key (available online) used to verify the digital signature. If A (the sender) and B (the receiver) are attempting to consummate an online transaction, B needs an independent confirmation that A's message is actually from A before B can have faith that A's public key actually belongs to A. It is possible that an imposter could have sent B the public key, contending that it belongs to A when in fact it does not. Accordingly, a reliable third party—the Certification Authority—must be available to register the public keys of the parties and to guarantee the accuracy of the identification of the parties (Hogan, 2000).

The most important job of the CA is to issue certificates which confirm basic facts about the subscriber, the subject of the digital certificate. The certificate is a digitized, computer-held record containing the most pertinent information about a transaction between two transacting parties: the name and address of the CA that issued the certificate; the name, address and other attributes of the subscriber;

the subscriber's public key; and the digital signature of the CA (Froomkin, 1996). Sufficient information will be contained in the certificate to connect a public key to the particular subscriber (Hogan, 2000).

In making an application to a CA for a certificate, the prospective subscriber must provide some sort of photo identification card, e.g., a passport or a driver's license. If the application is approved and the certificate is issued, the CA will issue a private key to its new subscriber which corresponds to the public key. This is done, however, without disclosing the specifics of the private key. The steps in this application procedure vary somewhat from CA to CA, according to the type of certificate being offered by the CA. Ordinarily, however, once the CA has verified the genuine connection between the subscriber and the public key, the certificate will be issued (Smedinghoff, 1999).

In order to indicate the authenticity of the digital certificate, the CA will sign it with his digital signature. Typically, the public key corresponding to the subscriber's private key will be filed in the CA's online repository which is accessible to the general public and to third parties who have need of communication with the subscriber. Additionally, the online repository contains information pertaining to digital certificates which have been revoked or suspended by the CA due to lost or expired private keys. This is an important positive aspect of PKI technology: the general public has access to the status of digital signatures, and relying third parties are kept informed, allowing them to judge whether they should place reliance on communications signed with a certain private key (Hogan, 2000).

One of the recurring problems for digital signature lawmakers is in trying to fairly apportion the liability for risk of computer fraud between the CA and the subscriber (Osty & Pulcanio, 1999). Nations around the world have arrived at different conclusions regarding this apportionment. The problem is compounded if each CA is required to modify its practices every time it issues a certificate pertaining to a transaction affecting another jurisdiction which happens to have dissimilar digital signature laws (Berman, 2001 and Maurushat, 2005).

A certificate is only as reputable as the CA that issues it. If the CA is unreliable and untrustworthy, the certificate is also unreliable and untrustworthy. In the final analysis, a party contracting with an unknown stranger must rely upon the CA's registration expertise and its judgment that the subscriber's identification is accurate (Hallerman, 1999).

THREE GENERATIONS OF E-SIGNATURE LAW

The First Generation of E-Signature Law: Technological Exclusivity

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law (Utah, 1995). In the Utah statute, digital signatures using PKI technology were given legal recognition, but other types of electronic signatures were not. Utah was not alone in this attitude; other jurisdictions granting exclusive recognition to the digital signature and PKI include Bangladesh, India (Blythe, 2006), Malaysia, Nepal (Blythe, 2008) and Russia (Fischer, 2001). 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 (Roland, 2001).

The Second Generation of E-Signature Law: Technological Neutrality

Jurisdictions in the Second Generation did the complete reversal of the First Generation and did not include any technological restrictions in their statutes. They did not insist upon the utilization of digital signatures, or any other form of technology, to the exclusion of other types of electronic signatures. These jurisdictions have been called "permissive" because they take a completely open-minded, liberal perspective on E-signatures and do not contend that any one of them is necessarily better than the others. Examples of permissive jurisdictions include the majority of states in the United States (Blythe, 2005 and 2008), the United Kingdom (Blythe, 2005 and 2008) Australia and New Zealand (Fischer, 2001). The disadvantage of the permissive perspective is that it does not take into account that the digital signature offers more security than other types of E-signatures (Blythe, 2009).

The Third Generation of E-Signature Law: A Hybrid

Singapore was in the vanguard of the Third Generation. In 1998, this country adopted a compromise position with respect to the various types of electronic signatures. Singapore's lawmakers were influenced by the UNCITRAL Model Law on Electronic Commerce (United Nations, 1996). Singapore adopted a "hybrid" model—a preference for the digital signature and PKI in terms of greater legal presumption of reliability and security, but not to the exclusion of other forms of electronic signatures. The digital signature is given more respect under the Singapore statute, but it was not granted a monopoly as in the first generation. This technological open-mindedness is commensurate with a global perspective and allows parties to more easily consummate electronic transactions with parties from other nations. Although granting legal recognition to most types of E-signatures, the Singapore statute makes a strong suggestion to users—in two ways—that they should use the digital signature because it is more reliable and more secure than the other types of E-signatures: (1) digital signatures employing PKI are given more status under rules of evidence in a court of law than other forms of electronic signatures, and E-documents signed with them carry a legal presumption of reliability and security—these presumptions are not given to other forms of E-signatures; and (2) although all forms of E-signatures are allowed to be used in Singapore, its E-signature law established comprehensive rules for the licensing and regulation of Certification Authorities, whose critical role is to verify the authenticity and integrity of electronic messages affixed to electronic signatures (Singapore, 1998).

In recent years, more and more nations have been joining the Third Wave. The hybrid, moderate position adopted by Singapore has now become the progressive trend in international E-signature law. The hybrid approach is the one taken by: the European Union's E-Signatures Directive (European Union, 1999); Armenia (Blythe, 2008); Azerbaijan (Blythe, 2007); Barbados (Blythe, 2006); Bermuda (Fischer, 2001), Bulgaria (Blythe, 2008); China (Blythe, 2007); Colombia (Blythe, 2010); Croatia (Blythe, 2008); Dubai (Blythe, 2007); Finland (Blythe, 2008); Hong Kong (Blythe, 2005); Hungary (Blythe, 2007); Iran (Blythe, 2006); Japan (Blythe, 2006); Lithuania (Blythe, 2007); Pakistan (Blythe, 2006); Peru (Blythe, 2010); Slovenia (Blythe, 2007); South Korea (Blythe, 2006); Taiwan (Blythe, 2006); Tunisia (Blythe, 2006); and Vanuatu (Blythe, 2006). Many other nations have adopted the hybrid approach. If Uganda enacts its Electronic Signature Bill, Uganda will become one of them.

UGANDA'S COMPUTER LAWS

Electronic Signature Bill

The Electronic Signature Bill is under consideration in Uganda (Uganda ESB, 2004-- hereinafter "ESB"). The ESB distinguishes an E-signature, an advanced E-signature, and a digital signature (Tang, 1999 and Poggi, 2000).

Fulfillment of Statutory Requirements

If a statute requires a handwritten signature, that requirement will be deemed to have been met if a reliable E-signature is attached to an E-document (ESB s 3(1)). The digital signature is the only type of E-signature one deemed to be sufficiently reliable (ESB s 3(2)).

Certification Authorities

Uganda's Minister of Communications ("Minister") appoints the Controller of Certification Authorities ("Controller"), who is responsible for regulation of Certification Authorities ("CA") (ESB s 20). All CA's must hold a license issued by the Controller (ESB s 21(1)). A CA is legally liable for ensuring that information on certificates (ESB ss 44-45 and 47-48) is accurate and for publishing of that information (ESB s 75); however, subscribers and relying third parties also have responsibilities (ESB ss 4, 6, 8). The ESB contains application procedures (ESB s 24), and a CA's license may be revoked if good cause exists (ESB s 26). A CA may also provide date/time stamp services (ESB s 78). All CA's must submit to an annual operational audit (ESB ss 37, 84-90) and are forbidden from engaging in activities which would increase the probability of loss to its subscribers (ESB s 79).

Crimes

It is a crime to: perform CA services without a license (ESB s 21(1)-(2)); violate one's duty of confidentiality of information after having obtained knowledge of the information pursuant to the ESB (ESB s 80(1)-(2)); make a false declaration pertinent to a legal requirement under the ESB (ESB s 81); and, as a corporate officer or director, to use a corporation to carry out a violation of the ESB (ESB s 82(1)-(2)). If the ESB does not provide for a specific punishment for a violation, then the general penalty will be applicable (ESB s 91(1)).

Electronic Transactions Bill

The Electronic Transactions Bill is also under consideration in Uganda (Uganda ETB, 2004--hereinafter "ETB"). The objectives of the ETB include: promotion of E-commerce and E-government; heightened security of E-transactions; and attainment of technological neutrality (ETB s 2(1)). The Minister of Communications is responsible for implementation of the ETB and may promulgate regulations to that effect (ETB s 33). The ETB is inapplicable to these types of documents: wills; testamentary trusts; powers of attorney; documents creating an interest and conveyance of an interest in real property which must be filed to apply to third parties; and negotiable instruments (including negotiable documents of title) (ETB s 3(1)). The ETB does not override any other law which explicitly authorizes, prohibits or regulates the use of E-documents (ETB s 3(2)). The ETB should be interpreted according to what is "commercially reasonable under the circumstances (ETB s 3(3))."

Fulfillment of Statutory Requirements

If a statute requires information to be in a paper document, that requirement will be deemed to have been met if the information is in an E-document, provided it is readily accessible for subsequent reference (ETB s 5). If a statute requires the presence of a handwritten signature on a paper document, that requirement will be deemed to have been met if an E-signature is attached to an E-document (ETB s 6). If a statute requires information to be produced or retained in its original form, that requirement will be deemed to have been met if the original information is produced or retained as an E-document, provided: the integrity of the information is maintained; and it may be accessed for reference by the person to whom it is presented (ETB s 7(1)-(2)). If a statute requires the storage of information or a document, that requirement will be deemed to have been met if an E-document is stored, provided: it is accessible for subsequent reference; it is stored in its original form, or one that reasonably depicts the information; the time/place of transmission/reception are indicated; and, if a government department requires the retention, that department has consented to use of the electronic form (ETB s 9(1)-(3)). If a statute requires the production of information or paper documents, that requirement will be deemed to have been met with production of an E-document, provided: the method of generation of the E-document reliably ensures its integrity (ETB s 10(2)); and the E-document is readily accessible for subsequent reference (ETB s 10(1)). If a statute requires a signed document to be notarized, that requirement will be deemed to have been met if the Notary Public's "advanced or secure electronic signature" is attached to an E-document which has the subscriber's E-signature also attached (ETB s 11(1)). If a statute requires the production of a certified copy of an E-document, that requirement will be deemed to have been met with production of a "printout certified to be a true reproduction of the document…" (ETB s 11(2)). If a statute requires the production of a certified copy of a paper document, that requirement will be deemed to have been met "if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature (ETB s 11(3))." If a statute requires multiple copies of a paper document to be delivered to one person at the same time, this requirement will be deemed to have been met if one E-document is sent to that person, provided: the E-document may be reproduced by that person (ETB s 12(1)). If a statute requires a seal to be affixed to a paper document, and the statute does not mention a method of electronic sealing, that requirement will be deemed to have been met with an E-document, provided: the E-document expresses that it is mandated to be under seal; and the advanced E-signature of the person by whom it is required to be sealed, is attached (ETB s 12(3)). If a statute requires or permits a paper document to be sent by registered/certified mail, that statute will be deemed to have been met if an E-document is sent to a service provider authorized by the Minister of Communications, is registered by that service provider and sent by the service provider to the E-mail address provided by the sender (ETB s 12(4)).

Admissibility and Evidential Weight

The ETB modifies the rules of evidence pertinent to authentication and best evidence (ETB s 8(1)(a)). Information in electronic form cannot be denied admission into evidence: (1) merely because of its form; or (b) if it is the best evidence, merely because it is not in its original form (ETB s 8(2)). The party seeking to have an E-document admitted into evidence has the burden of proving the E-document's authenticity, which requires a showing that the document is what the person claims it to be (ETB s 8(3)). If the best evidence rule is applicable, the party introducing an E-document must prove the integrity (ETB s 8(6)) of the computer information system in which the E-document was recorded or retained (ETB s 8(4)). Factors for the court to consider in determination of the evidential weight of an E-document include: the reliability of the computer information system; the reliability of methods used to maintain the integrity of the E-document; and the method used to identify the sender or retainer of the E-document (ETB s 8(5)).

E-Contracts

The legal validity of information in an E-message cannot be denied merely because of its electronic form (ETB s 4(1)). A contracting party may express his intent electronically (ETB s 17). An E-contract is legally valid (ETB s 15(1)). The E-contract comes into existence at the time and place that the offeror receives the acceptance from the offeree (ETB s 15(2)); there would be no "Mailbox Rule" as in the United States. For information incorporated by reference to become part of an E-contract, it must be: (1) referenced in such a manner that a reasonable person would have noticed it and incorporated it; and (2) accessible for the other party to read, retain and retrieve it, either in electronic form or in a physical printout (but the information must be capable of reduction to electronic form by the party incorporating it) (ETB s 4(2)). Commonplace rules are provided for: automated transactions (ETB s 13); time and place of transmission and receipt (ETB ss 16(1)-(6) and 19); and attribution (ETB s 18).

Consumer Protections for E-Buyers

An E-seller must post complete and accurate information at its website to potential E-buyers, including: its identity; membership in accrediting organizations; its code of conduct; number and address of registration; officers; descriptions of goods and services offered; price, payment method, terms of agreement and delivery time; manner used to access a record of the transaction; exchange and refund policy; alternative dispute resolution method; privacy policy and security procedures used; and minimum duration of the agreement (if it an ongoing contract) (ETB s 23(1)). After placing an order, but before it becomes final, the E-buyer must be allowed to review the order in order to correct any mistakes or to cancel the order (ETB s 23(2)). The E-seller is required to execute the order within thirty (30) days after its receipt, unless the parties have made a contrary agreement (ETB s 26(1)). If the seller fails to do so, the buyer may cancel the contract after giving the seller seven (7) days' written notice (ETB s 26(2)). If the seller is unable to complete the contract because of unavailability of the goods, then the seller must immediately inform the buyer and refund all payments made within thirty (30) days of that notification (ETB s 26(3)).

If the E-seller fails to comply with the obligations stated in the preceding paragraph, the E-buyer may cancel the order within fourteen (14) days after receipt of the goods and services (ETB s 23(3)). This is a noteworthy provision; the ETB would grant the E-commerce buyer some of the best protections in the world. If cancellation occurs, the E-buyer must return the goods or stop using the service. Whereupon, the seller must refund all payments to the buyer less any transportation and handling cost incurred by the seller in return of the goods (ETB s 23(4)).

The E-seller is required to use a secure payment system (ETB s 23(5)). If the E-seller fails to do so, it is liable for any pertinent damages incurred by the E-buyer due to the insecure system (ETB s 23(6)). The aforementioned consumer protections are inapplicable to: financial and investment service transactions; auctions; purchases of food and drink to be ordinarily consumed at a worksite or at home; services beginning with the consumer's consent before the end of the seven (7) day period mentioned in the next paragraph; transactions in which the price is dependent on the vagaries of the financial markets; custom-made goods; perishable goods; audio/video recordings or software that has been unsealed by the consumer; reading materials; gambling; and when the transaction relates to "accommodation, transport, catering or leisure services" and the E-seller has agreed to provide them on a date certain or during a period certain (ETB s 23(7)).

An E-buyer may cancel the contract within seven (7) days of receipt of the goods, on in a service contract, within seven (7) days of the date the contract was consummated (ETB s 24(1)). If payment has already been made, the buyer is entitled to a full return of the amount paid (ETB s 24(3)), less any transportation and handling charges incurred by the seller in return of the goods (ETB s 24(2)). These provisions do not prejudice any consumer right created by other laws (ETB s 24(4)).

If a party sends unsolicited advertisements to a consumer by E-mail, the receiver must be given the option of removing his name from the mailing list and must be informed the source from which the party obtained the consumer's name and E-mail address (ETB s 25(1)). If the offending party fails to do so, he is punishable with a maximum fine of 1,440,000 shillings and/or three years' imprisonment (ETB s 25(2)). If the party continues to send unwelcome E-mail advertisements after being advised not to do so, he may be punished further with an additional fine of 1,440,000 shillings and/or three years' imprisonment (ETB s 25(3)).

The aforementioned consumer protections will be effective irrespective of whether domestic or foreign law governs the interpretation of the contract (ETB s 27). The aforementioned consumer protections may not be avoided by agreement of the parties (ETB s 28).

Liability of Internet Service Providers

As a general rule, an internet service provider is not criminally or civilly liable for mere dissemination of infringing or offensive material on behalf of another party (ETB s 29(1)-(2)), or merely providing a link whereby a user may obtain access to infringing or offensive material (ETB s 30). There is no general obligation to monitor the material which is disseminated over the internet by the service provider (ETB s 32). If a person believes offensive or infringing material is being disseminated by the service provider, that person should give written notice to the service provider (ETB s 31).

E-Government

A government department may elect to accept or issue E-documents or E-payments (ETB s 20). The implementation of E-government is not mandatory. If it elects to offer E-government services, format and other requirements may be specified by each department (ETB s 21).

Computer Misuse Bill

The Computer Misuse Bill is also under consideration in Uganda (Uganda CMB, 2004—hereinafter, "CMB"). The CMB would prohibit: obtaining unauthorized access to a computer (CMB s 9); obtaining unauthorized access to a computer for the purpose of commission of a further crime (CMB s 10); obtaining a computer access code without authorization (CMB s 14); violation of one's duty to maintain confidentiality of information obtained pursuant to the CMB (CMB s 15); use of a computer to access, obtain, disseminate or sell child pornographic material (CMB s 18); and acts of aiding or abetting the commission of the aforementioned crimes (CMB s 17). More stringent punishments are provided for if the computer is "protected" (CMB s 16). Law enforcement authorities are authorized to conduct search-and-seizure operations in furtherance of enforcement of the CMB (CMB s 19), and the CMB would provide for "long arm" jurisdiction over offending foreign parties (CMB s 21).

SUMMARY: UGANDA'S COMPUTER LAWS

The ESB is third-generation and provides for compulsory licensing of CA's. The ETB contains ordinary E-contract rules for automated transactions, attribution, acknowledgement of receipt, and time/place of transmission/reception; and ordinary E-government and internet service provider rules are listed. One of the ETB's distinguishing positive aspects concerns fulfillment of statutory requirements relating to notarization, certification, and contract under seal. However, the most impressive portion of the ETB is its comprehensive list of consumer protections for E-commerce buyers: required information of the E-seller to be listed at its website; final review of agreement by buyer before consummation; 14-day window to cancel the contract if the information or final review is not given; utilization of a secure payment system by seller, with seller liable to buyer for damages caused by its failure thereof; 7-day, "no-questions-asked" window to cancel the contract after it has been consummated, with buyer merely having to return goods to seller; and prohibition against sending unsolicited E-mail advertising to a consumer after being asked to cease doing so.

The CMB is a good computer crimes law It is similar to Singapore's Computer Misuse Act (Singapore, 1993) and is potentially far-reaching because it provides for "long arm" jurisdiction.

RECOMMENDATIONS FOR IMPROVEMENT OF UGANDA'S PROPOSED COMPUTER LAWS

Electronic Signature Bill

Add Reciprocal Recognition of Foreign CA's and Certificates Issued by Foreign CA's

Most international E-commerce laws now provide for various forms of legal recognition of foreign CA's and certificates issued in foreign countries, the ESB fails to do this. This is essential because E-commerce transactions often straddle international borders. Turkey's Electronic Signature Law is a typical example and can be used as a model (Turkey, 2004).

Assign More Potential Liability to CA's

It is unusual in international E-signature law to find as much limitation of a CA's liability as in Uganda. This needs to be changed. Too much responsibility is placed upon the shoulders of the subscriber, and too little responsibility is assigned to the CA. Some of the burden of potential liability should be transferred from the subscriber to the CA. The computer law of the Republic of Vanuatu can be used as a model (Vanuatu, 2000).

Electronic Transactions Bill

Information Technology Courts

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology ("I.T.") Courts should be established as a court-of- first-instance for them. The I.T. Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in E-commerce law, and the other two persons would be an I.T. expert and a business management expert. The attorney would be required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field; and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The E-commerce law of Nepal can be used as a model (Nepal, 2005).

Mandatory E-Government

In order to reduce cost and to make governmental functions more convenient for citizens, E-government needs to be emphasized and mandated. By established deadlines, governmental departments should begin to convert to provision of online services if possible. In Hong Kong, for example, a substantial number of government services may now be accessed online, e.g., the scheduling of an interview for a visa or the scheduling of a wedding before a public official (Chung, 2003).

Eliminate the Exclusion for Wills

The ETB excludes wills from its coverage. The result is that a will is required to be in paper form with a handwritten signature affixed to it in order to be enforceable. This exclusion should be eliminated. Electronically-signed wills should be recognized. There is evidence that the aversion to electronic wills is beginning to dissipate. 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 (Ross, 2005).

Computer Crimes Bill

The following crime should be added to the CCB: Intentional Injection of a Virus Into a Computer System. This crime is especially heinous because of its potential for infliction of extreme damage to the Ugandan economy as well as to the international economy. The punishment should be stringent, as follows: first offense, mandatory ten years' imprisonment, without parole; second offense, mandatory twenty years' imprisonment, without parole; and third offense, mandatory life imprisonment, without parole.

REFERENCES

American Bar Association ("A.B.A.") (1995-96), Section of Science & Technology, Information Security Committee, Electronic Commerce & Information Technology Division, *Digital Signature Guidelines*, p. 9; http://www.abanet.org/ftp/pub/scitech/ds-ms.doc .

American Bar Association ("A.B.A.") (2001), *PKI Assessment Guidelines (Public Draft for Comment No. 25)*, V 0.30 at 301 and 305; http://www.abanet.org/scitech/ec/isc/pagv30.pdf. Under the proposed Ugandan law, the private key is defined as "the key of a key pair used to create a digital signature." ESB, section 1. The "key pair" is defined as "a private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates." *Id.* Under the proposed Ugandan law, a public key is defined as "the key of a key pair used to verify a digital signature and listed in the digital signature certificate." *Id.* The private key and the public key are examples of what the proposed Ugandan law refers to as electronic-signature products—"configured hardware or software, or relevant components thereof, which are intended to be used by a [Certification Authority] for the provision of electronic signature services *or are intended to be used for the creation or verification of electronic signatures*." *Id.* (Emphasis added.)

Antigua and Barbuda (2006). *Electronic Transactions Act*.

Bahamas, Commonwealth of (2003). *Electronic Communications and Transactions Act.*

Banks, Amanda (24 July 2009). E-Commerce Solutions Continue to Flourish in Caribbean. *Tax-News.Com*, London.

Barbados (8 March 2001). *Electronic Transactions Act, Cap. 308B*.

Berman, Andrew B. (2001). Note, International Divergence: The 'Keys' To Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures. *Syracuse Journal of International Law and Commerce*, 28, 125.

Blythe, Stephen E. (2008). Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security. *Armenian Law Review*.

Blythe, Stephen E. (2007). Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region. *Columbia Journal of East European Law*, 1, (1), 44-75.

Blythe, Stephen E. (2006). The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute. *Caribbean Law Review*, 16, (1).

Blythe, Stephen E. (2008). Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce With Secure Cyber-Transactions. *Transnational Law and Contemporary Problems*, 17, (2), 361.

Blythe, Stephen E. (2007). China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce. *Chicago-Kent Journal of Intellectual Property*, 7, (1).

Blythe, Stephen E. (2010). Computer Law of Colombia and Peru: A Comparison With the U.S. Uniform Electronic Transactions. *Internet Policies and Issues*, Chapter 2 (New York: Nova Science Publishers, Inc., Frank Columbus, Ed.).

Blythe, Stephen E. (2008). Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber-Security. *European Journal of Law and Economics*, 26, (1), 75-103.

Blythe, Stephen E. (2007). The Dubai Electronic Transactions Statute: A Prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries. *Journal of Economics and Administrative Sciences*, 22, (1), 103.

Blythe, Stephen E. (May, 2008). E-Signature Law and E-Commerce Law of the European Union and its Member States. *The Ukrainian Journal of Business Law*, pp. 22-26.

Blythe, Stephen E. (2008). Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services. *Hamline Law Review*, 31, (2), 445-469.

Blythe, Stephen E. (2005). Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World's "Most Wired" City. *North Carolina Journal of Law and Technology*, 7, 1.

Blythe, Stephen E. (2007). Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions. *Information and Communications Technology Law*, 16, (1), 47-71.

Blythe, Stephen E. (2006). A Critique of India's Information Technology Act and Recommendations for Improvement. *Syracuse Journal of International Law and Commerce*, 34, 1.

Blythe, Stephen E. (2006). Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World. *Sri Lanka Journal of International Law,* vol.18.

Blythe, Stephen E. (2006). Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access. *Journal of Internet Law*, 10, 20.

Blythe, Stephen E. (2006). The Tiger on the Peninsula is Digitized: Korean E-Commerce Law as a Driving Force in the World's Most Computer-Savvy Nation. *Houston Journal of International* Law, 28, (3), 573-661.

Blythe, Stephen E. (2007). Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions. *Barry Law Review*, 8, 23.

Blythe, Stephen E. (2008). On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law. *Journal of High Technology Law,* 8, 1.

Blythe, Stephen E. (2006). Pakistan Goes Digital: the Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce. *Journal of Islamic State Practices in International Law*, 2, (2), 5.

Blythe, Stephen E. (2006). Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality. *Ohio Northern University Law Review*, 33, 525-562.

Blythe, Stephen E. (2007). Slovenia's Electronic Commerce and Electronic Signature Act: Enhancing Economic Growth With Secure Cyber-Transactions. *The I.C.F.A.I. Journal of Cyber Law*, 6, (4), 8-33.

Blythe, Stephen E. (2006). Taiwan's Electronic Signature Act: Facilitating the E-Commerce Boom With Enhanced Security. *Proceedings of the Sixth Annual Hawaii International Conference on Business*.

Blythe, Stephen E. (2006). Computer Law of Tunisia: Promoting Secure E-Commerce Transactions With Electronic Signatures. *Arab Law Quarterly*, 20, 317-344.

Blythe, Stephen E. (May 19-23, 2009). The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control. *Proceedings of the Tenth Annual Conference of the International Academy of African Business and Development*, Kampala, Uganda.

Blythe, Stephen E. (2005). Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security. *Richmond Journal of Law and Technology*, 11, (2), 6.

Blythe, Stephen E. (November, 2008). E-Commerce and E-Signature Law of the United States of America. *The Ukrainian Journal of Business Law*.

Blythe, Stephen E. (2006). South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga. *Journal of South Pacific Law*, 10, (1).

Chung, Rina C.Y. (2003). Hong Kong's 'Smart' Identity Card: Data Privacy Issues and Implications for a Post-September 11th America. *Asian-Pacific Law and Policy Journal* 4, 442. In the highly successful Hong Kong Identity Card, the two thumb prints are used as a biometric identifier. *Id*.

Dessent, M. (2002). Browse-Wraps, Click-Wraps and Cyberlaw: Our Shrinking (Wrap) World. *Thomas Jefferson Law Review* 25, (1), 4.

European Union ("E.U.") (1999), *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures*, (1999/93/EC)—19 January 2000, OJ L OJ No L 13, p.12.

Fischer, Susanna Frederick (2001). California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation. Association of American Law Schools 2001 Annual Meeting, Section on Law and Computers, *Boston University Journal of Science and Technology Law*, 7, 229-237.

Froomkin, A. Michael (1996). The Essential Role of Trusted Third Parties in Electronic Commerce. *Oregon Law Review*, 75, 49-58 (1996).

Hallerman, D. (1 June 1999). Will Banks Become E-commerce Authorities? *Bank Technology News*, v. 12.

Hogan, T. C. (2000), Notes and Comments—Technology, Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business? *North Carolina Banking Institute* 4, 424-27. Under the proposed Ugandan law, a Certification Authority is defined as "a person who issues a certificate." ESB section 1. Under the proposed Ugandan law, a certificate is defined as "a computer-based record which—(a) identifies the certification authority issuing it; (b) names or identifies its subscriber; (c) contains the subscriber's public key; and (d) is digitally signed by the certification authorit6y issuing it." *Id.*

Hong Kong Special Autonomous Region (2000). *Electronic Transactions Ordinance*, Ord. No. 1 of 2000, Section 2. The Hong Kong E-commerce law typically defines a digital signature as follows: "an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine: (a) whether the transformation was generated using the private key that corresponds to the signer's public key; and (b) whether the initial electronic record has been altered since the transformation was generated." *Id.*

Maurushat, A. (2005). *Hong Kong Law Journal* 35, (3), 569. This argued contended that multi-lateral recognition of Certification Authorities among China, Hong Kong and Singapore should only occur after their PKI legislation has been harmonized and each of them provides sufficient privacy protections for personal data.

Nepal (2005), *Electronic Transactions Ordinance No. 32 of the Year 2061 B.S.,* ss 60-71.

Osty, M.J. and Michael J. Pulcanio (1999). The Liability of Certification Authorities to Relying Third Parties. *John Marshall Journal of Computer and Information Law* 17, 961.

Poggi, C.T. (2000). Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation. *Virginia Journal of International Law* 41, 224. Under the proposed Ugandan law, a digital signature is defined as "a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine—(a) whether the transformation was created using the private key that corresponds to the signer's public key; and (b) whether the message has been altered since the transformation was made." ESB section 1. Furthermore, under the proposed Ugandan law, the digital signature also complies with the requirements contained in the definition of an "Advanced" Electronic Signature: "an electronic signature, which is uniquely linked to the signatory; is reliably capable of identifying the signatory; is created using secure signature creation device that the signatory can maintain under his sole control; and is linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and the signature are detectable." *Id.* In the ESB, a signatory is defined as "a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents." *Id.*

Pun, K.H., Lucas Hui, K.P. Chow, W.W. Tsang, C.F. Chong & Felix Chan (2002). Review of the Electronic Transactions Ordinance: Can the Personal Identification Number Replace the Digital Signature? *Hong Kong Law Journal*, 32, 243-256.

Roland, Sarah E (2001). The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?. *Suffolk University Law Review*, 35, 638-45.

Ross, Chad Michael (2005). Comment, Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will. *University of Memphis Law Review*, 35, 603.

Singapore, Republic of (1993), *Computer Misuse Act* (Cap. 50A).

Singapore, Republic of (1998). *Electronic Transactions Act* (Cap. 88).

Smedinghoff, T.J. (1999). Electronic Contracts: An Overview of Law and Legislation. *PLI/P*, 564, 125-162.

Stern, J.E. (2001). Note, Federal Legislation: The Electronic Signatures in Global and National Commerce Act. *Berkeley Technology Law Journal*, 16, 395.

Tang, D.K.Y. (1999). Electronic Commerce: American and International Proposals for Legal Structures. *Regulation and Deregulation Policy and Practice in the Utilities and Financial Services Industries* (Chrisopher McCrudden, Ed.), 333.

Tonga, Kingdom of (2003), *Computer Crimes Act*.

Tunisia, Republic of (2000). *Electronic Exchanges and Electronic Commerce Law,* art. 25-37.

Turkey, Republic of (2004). *Electronic Signature Law,* art. 14.

United Arab Emirates (2006). *Federal Law No. 1 of 30 January 2006 on Electronic Commerce and Transactions*.

.

United Nations, Commission on International Trade Law (1996). *Model Law on Electronic Commerce With Guide To Enactment*, G.A. Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, p. 336, U.N. Doc. A/51/49.

United States of America (1998). *Uniform Commercial Code*, Sections 2-201 and 2-209.

Uganda, Republic of (2004), *Computer Misuse Bill* (hereinafter “CMB”); http://www.sipilawuganda.com/downloads/computer%20misuse%20bill.pdf.

Uganda, Republic of (2004), *Electronic Signatures Bill* (hereinafter “ESB”); http://www.sipilawuganda.com/downloads/electronic%20signatures%20bill%202004.pdf.

Uganda, Republic of (2004), *Electronic Transactions Bill* (hereinafter “ETB”); http://www.sipilawuganda.com/downloads/electronic%20transactions%20bill.pdf.

Utah, State of (1995), *Utah Code Annotated* 46-3-101 *et seq*.

Vanuatu, Republic of (2000). *Electronic Transactions Act* s 23(1)(a)-(c).

Zaremba, J. (2003). International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers. *Connecticut Journal of International Law*, 18, 479-512.