JOAAG

As_Saber, Srivastava & Hossain, 2006 Information technology law and e-government: A developing country perspective. *JOAAG*. Vol. 1. No. 1

Information Technology Law and E-government: A Developing Country Perspective[1]

Sharif N As-Saber[2]

Aashish Srivastava[3]

Khalid Hossain[4]

Abstract

In recent years, there has been a worldwide wave of using e-government as a mechanism to improve government's efficiency through transparency, openness and increasing interactions across governments, citizens, and the civil society organisations. However, Bangladesh has failed to progress towards achieving its target as envisaged in its information technology (IT) policy documentations. The inability of the national parliament to enact an IT law is primarily considered responsible for such a failure. This paper initially attempts to identify issues relevant to the use of information and communication technology (ICT) and e-government in Bangladesh. It is followed by a discussion on the legal aspects of the use of ICT in e-government activities and the country's failure to enact the draft IT Act for more than four years. Subsequently, a framework of e-government and legal protection is introduced and major ICT related legal issues discussed with references to the draft IT Act of Bangladesh and other relevant legal codes

Key words: e-government, IT Act, developing country perspective, Bangladesh

[1] The earlier version of this paper was presented to a research conference on the practice of e-government and e-governance organised by Monash University in June 2006.

[2] Senior Lecturer at the Department of Management, Monash University, Melbourne.

[3] Doctoral Candidate at the Department of Business Law & Taxation, Monash University, Melbourne

[4] Research Officer at Bangladesh Tariff Commission, Dhaka

Introduction

Governments all over the world have started resorting to the newly found information and communication technology (ICT) to establish a citizen-centric, more transparent and more accountable government mechanism. Available ICT infrastructures together with government's willingness to implement e-governance have already brought success in e-government initiatives across the industrialised world (Robins & Burn, 2001). While some developing countries have taken steps in this regard, they often fall short of expectations in improving their governance structure and relevant outcomes. In this regard, a number of barriers exist that need to be understood and tackled by developing countries in pursuing e-government objectives. These include, lack of ICT resources and infrastructure such as high-speed broadband network connections, unequal access to technology (resulting into 'digital divide'), low literacy rate, corruption and the lack of government policy initiatives. Often, 'the lack of resources and technology is compounded by a lack of access to expertise and information' (PCIP, 2002: 1). A strong political will and commitment, reflected in a country's politico-legal structure, are in the core of combating these barriers and achieving success. Together with other laws of the land, the presence of a well-orchestrated IT Act could provide the necessary foundation and benchmark in this regard and facilitate the smooth functioning of a country's ICT sector. It may also function as a safeguard to all ICT related activities including e-government bolstering trust and confidence across the various stakeholders of e-government, viz., the government, citizens, businesses and the members of the wider civil society including non-government organisations (NGOs).

As a least developed but emerging economy, Bangladesh has been struggling to improve its government structure. Marred by corruption, political division, inefficient bureaucratic practices, it has been a difficult task for the government of Bangladesh to put the country on the right development path (Jamil, 2002). However, the country has been endeavouring to implement e-government in recent years to improve its current administrative practices and to establish a better relationship and transparency between the government and its various stakeholders (MOSICT, 2006). In order to achieve this objective, the government formulated its ICT policy in 2002. The policy emphasises that in order to meet these objectives an appropriate IT legislation "…should

be enacted immediately". More than four years have elapsed since the ICT policy warranted an ICT Act but no such legislation has been passed to date. Cabinet approved the draft ICT Act in early 2005 but it is yet to become a law as the national parliament has failed to enact it (Parveen, 2006; "Cabinet okays," 2005). In the absence of such Act, businesses and citizens remain wary and hesitant to get involved in any electronic communication and transactions. It also makes cyber crimes and other ICT-related irregularities extremely difficult to combat and privacy and security become hard to ensure in electronic communication and transactions. Offences such as threat to life and property via email, wrongful loss or damage via computer viruses, etc. are still dealt with traditional criminal laws which are not considered sufficient enough to address the unique nature of internet-based criminal activities (Parveen, 2006).

This paper initially attempts to identify issues relevant to the use of ICT and e-government in Bangladesh. It is followed by a discussion on the legal aspects of the use of ICT in e-government activities and the country's failure to enact the draft IT Act for more than four years. Subsequently, a framework of e-government and legal protection will be introduced and major ICT related legal issues will be discussed with references to the draft IT Act of Bangladesh[1] and other existing legal codes.

ICT and e-government in Bangladesh

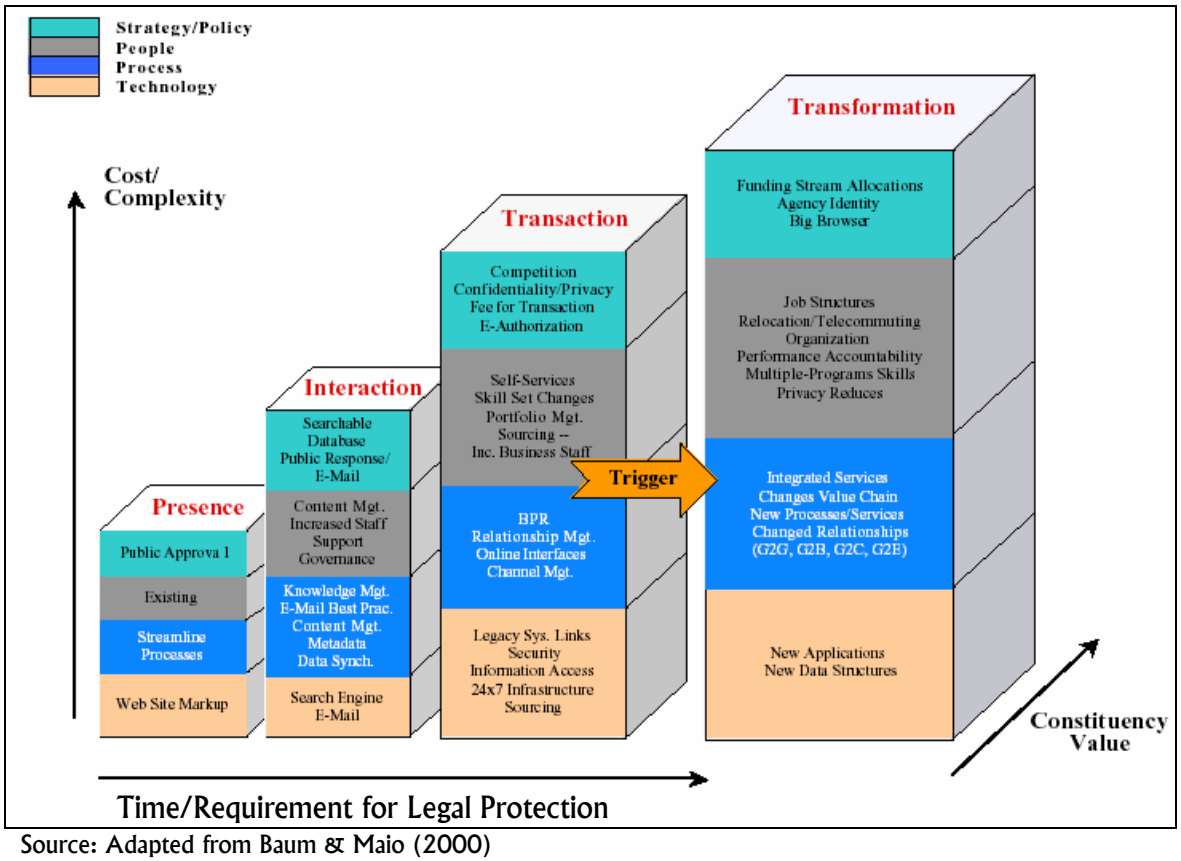
The ICT Policy 2002 aimed at 'building an ICT-driven nation comprising of knowledge-based society by the year 2006' (MOSICT, 2002). However, Bangladesh has failed to achieve its ICT target as enunciated in the ICT Policy. In the area of e-government, the achievements fell significantly short of the expectations. Using 'Gartner's Four Phases E-Government Model,' it is possible, to a certain extent, to determine the progression of e-government in Bangladesh.

In 2000, the Gartner Group Inc formulated a schema identifying four phases of e-government in order to measure the progression of e-government and identified strategy and other factors contributing to a country's success in each phase (see Figure 1). The model suggested the four critical phases of e-government evolution, viz., the web presence, interactions, transactions and transformation. At the moment, Bangladesh

[1] The Draft Act has been sourced from the website of Bangladesh Law Commission, http://www.lawcommissionbangladesh.org/wplit.pdf

appears to be at the second phase of e-government. However, the public response to the e-government is lukewarm and without much enthusiasm. There are hardly any electronic service deliveries by government and joined-up government is still a far-reaching goal in Bangladesh. In the absence of a comprehensive IT Act, many issues including the privacy and security remain unresolved making it difficult for Bangladesh to reach the third phase of e-governance. Although most of the government organisations in Bangladesh have developed their web presence with information about their respective organisations and their activities, the level of e-service delivery remains limited.

Figure 1: Gartner's Four Phases of E-Government Model and the Necessity for a Legal Protection



Source: Adapted from Baum & Maio (2000)

As suggested by Gartner's Model (Figure 1), the third and the fourth phases are significantly more complex and much more expensive to implement. As the levels of cost and complexity are incremental so are the risks and loopholes in relation to new techniques and technologies associated with the higher stages. Innovative e-government procedures together with complex ICT structure could be threatened by increasingly innovative techniques of web piracy and hacking. An appropriate level of legal

protection is considered vital to minimise such risks. The legislation of a sound IT Act dealing with all such loopholes is a primary precondition to switch to a more constituent-driven and extensive new phase of e-government.

Legal issues of e-government

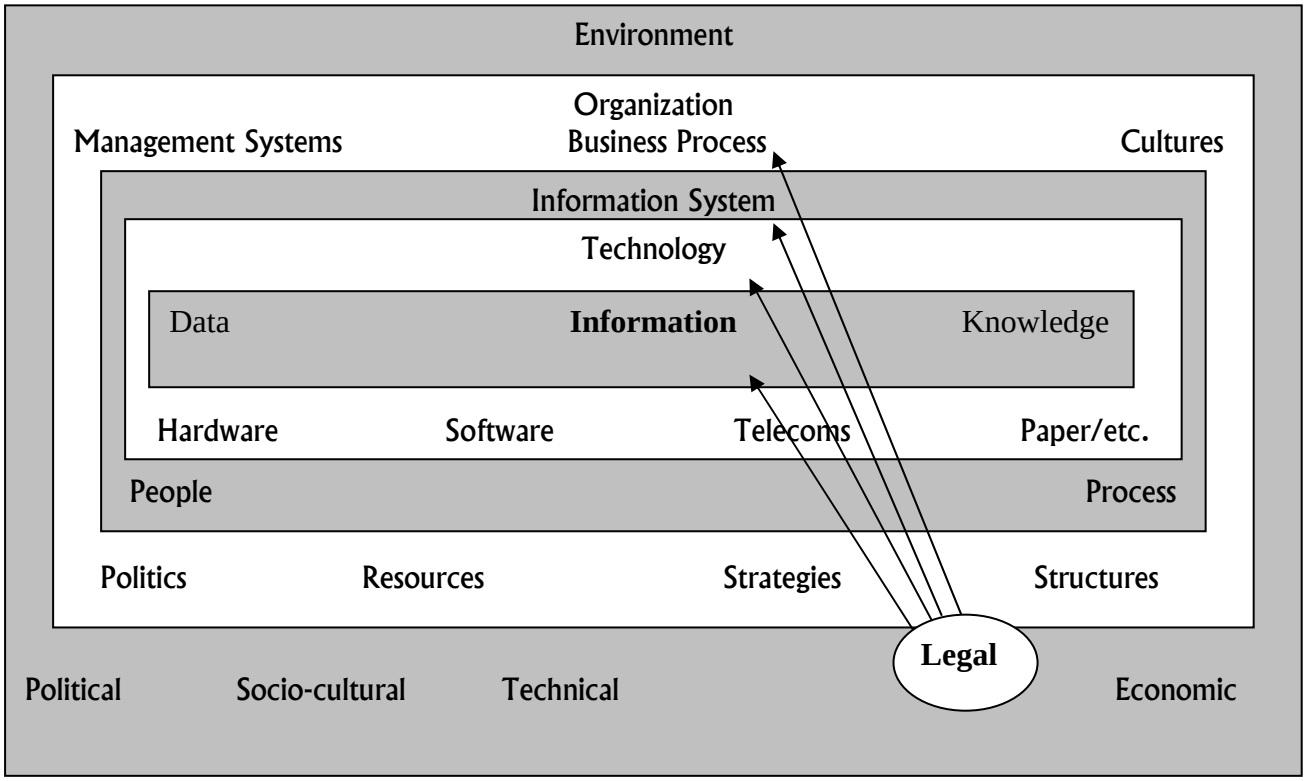
Seamless communication and information flow and data management are the primary preconditions of an effective e-government structure. It requires reasonable assurance of not being affected by illegal activities undertaken by computer hackers and cyber criminals. In this regard, it is important that sufficient safeguards are in place in order to ensure security and privacy of information and data management. Therefore, a strong administrative framework together with the ability to enforce law is an important precondition for a country's economic development and stability. Appropriate law needs to be enacted to address the legal needs of specialized, complex and highly technical ICT sector. Any obstacles, either legal or administrative, may hinder the implementation and progression of e-government activities (Caine, 2004).

A country must prepare itself in order to overcome any such obstacles and embrace e-government. In this regard, Bhatnagar (2004, p. 74) opines, a country becomes ready to adopt e-government when there is an 'existence of an enabling legal framework encompassing privacy and security of data, legal sanction of new forms of storage and archiving, and laws that accept paperless transactions'.

Dave (2005) argues the lack of authenticity and reliability, lack of accountability, redundancy of data, improper identification of user such as citizens, lack of accountability due to inappropriate delegation of authority, cyber crimes like fraud, theft, virus and incompetent security of on-line data transaction on Internet are the leading barriers to implement e-government from a legal perspective. Dave (2005) further argues, as 'governance' itself is a term used to imply public administration through government mechanisms under laws and conventional procedures, 'e-governance' could not be conceptualised from an alien perspective by ignoring the basic theme of governance. Legal provisions are, therefore, important in e-government to have citizen's faith and confidence on government system, to avoid vulnerability of electronic system from cyber crimes and to have acceptance from targeted groups of e-governance (Dave, 2005). From an overall e-government perspective, Figure 2

demonstrates how the legal issue becomes an important environmental factor affecting all major layers of the e-government framework.

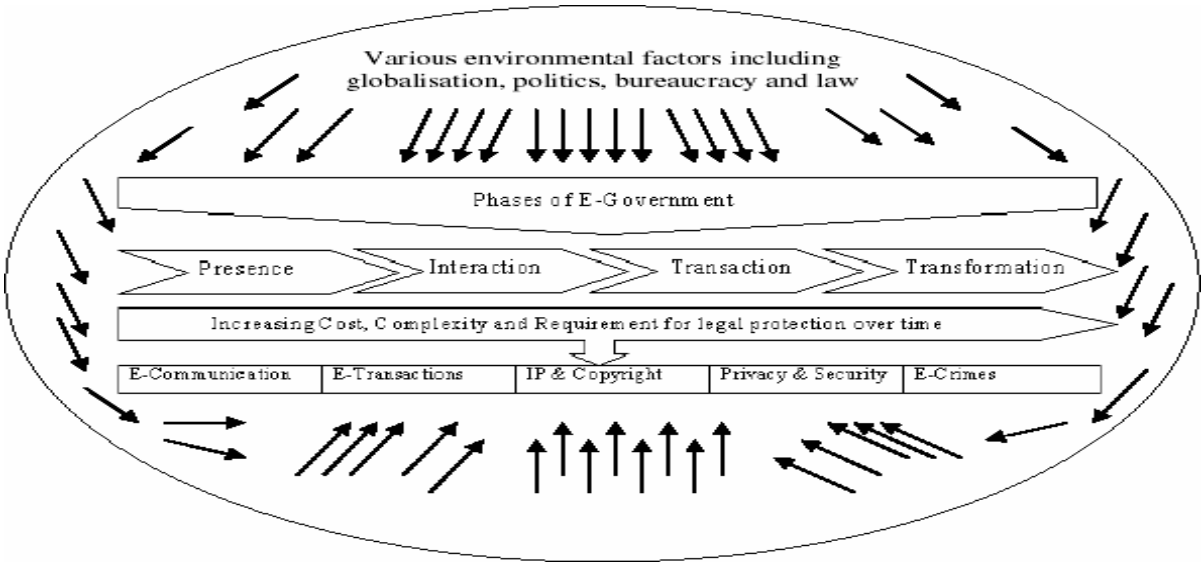
Figure 2: Presence of legal issue in a complete model of E-government



Burkert (2004) considers legal aspects of any public sector information system as the core requirement of a successful e-government framework. As e-government provides government services to citizen mainly through Internet as the electronic information media, Kubicek (2004) argues that e-government requires freedom of information as it is linked with information and knowledge society. However, while providing information through website in its e-government initiative, a government organization might provide written materials, images, music and audio-visual material. All of these materials might be protected through copyright law. Moreover, databases and softwares used in the web page, and even the design of a web page might be protected under intellectual property law (Veysey, 2004). Hence, while providing public sector information, violation of intellectual property law might occur whether intentionally or not. If government tries to monopolize information resources in its e-government process, there might be conflict with private sector partners under a competition law regime regarding the extent government could have control over public sector information (Burkert, 2004).

Schartum (2004) also thinks that an open government related with the concept of e-government has both legal and political aspects to be considered. A single issue related with e-government, access to information, needs a legal blend of three separate acts like freedom of information act, personal data act and administrative procedure act (Schartum, 2004). Based on the discussion above, a tentative framework of e-government and legal protection could be drawn (Figure 3).

Figure 3: E-government and Legal Protection



Based on Gartner's four phases of e-government (Baum & Maio, 2000), the framework suggests, as complexity and costs increase while moving from one phase to another, the need for legal protection becomes increasingly important in the transition process. The improvement of the constituency value, therefore, relies on a stable and effective e-government structure backed by adequate legal protection. The major areas of e-government that require legal protection are e-communication, e-transactions, intellectual property (IP) & copyright, privacy and security and e-crimes.

E-government and legal protection: The Bangladesh context

While discussing the e-government in Bangladesh, Taifur and Chowdhury (2003) observe that the government system in Bangladesh resistant to the use of IT in public services as it is assumed that the use of IT would diminish the power of the public service. The absence of a legally binding IT Act has made the situation worse and further complicated. Despite enshrining ICT as an important sector in the ICT Policy documents of Bangladesh, the ICT as a governance tool is yet to be used extensively. In

this regard, legislation of an IT Act is way overdue. A speedy legislation of an IT Act was recommended in the ICT Policy (MOSICT, 2002), which is yet to be achieved. Without its enactment, it is not possible for Bangladesh to enter the 'transaction' phase, the third phase of e-government progression, which specifically emphasise on the security and privacy issues. Even in the current phase, the country will continue facing problems associated with cybercrimes including any illegitimate use of Internet and computers.

As laid down in the above-mentioned framework of e-government and legal protection (Figure 3), the five areas of e-government that require legal protection are discussed below from the Bangladesh perspective. The provisions within the draft IT Act are acknowledged and the prevailing legal underpinnings are mentioned to appraise the current legal fabric of e-government.

E-Communication

Communication matters and the primary thrust of e-government is to develop and maintain an effective e-communication protocol between the government and citizens and across and beyond government agencies. In legal terms, e-communication includes attribution, acknowledgement and dispatch of electronic records that has been dealt with in the Draft IT Act of Bangladesh (§s 12 to 14). The three sections in the Act are adopted verbatim from the UNCITRAL Model Law on Electronic Commerce 1996. §12 lays down the various conditions under which an electronic record is attributable to its originator. For example, an electronic record is deemed to be that of the originator if it is sent by a person acting on behalf of the originator or by an information system programmed by or on behalf of the originator. § 12 also lays down provisions under which the addressee is entitled to assume that an electronic record is that of an originator and acts on that assumption. The provisions with regard to time, place and receipt of electronic records are laid down in § 14. It states that unless agreed otherwise between the originator and the addressee (for which provisions are laid down in §13) the dispatch of an electronic record occurs when it reaches a computer resource beyond the control of the originator. This means that the moment an e-mail sent by the originator leaves the originator's computer and resides on an intermediate server, it can be said that the electronic record has been dispatched by the originator. §14 further states that where the addressee has designated a specific computer resource

to the originator for receiving the electronic record, the time at which the electronic record enters the designated computer resource shall be deemed to be the time of receipt of the electronic record. However, in the case where the addressee has not designated any such resource the time of receipt shall be the time when the electronic record enters the computer resource of the addressee. § 14 also deals with the place of business and states that the place where the electronic record is sent or received shall be deemed to be the place of business of the originator and addressee respectively. However, in the absence of the place of business, originator's and addressee's usual place of residence shall be deemed to be the place of business. § 14 provides an overriding clause that the parties may agree otherwise on the place of sending and receipt of electronic record and in such a case the agreement will prevail over the provisions of the section.

As the Act is yet to be approved by the national parliament, the legal status of e-communication remains in disarray. The Bangladesh Telecommunication Act 2001 recognises Internet as a telecommunication service. However, it does not have a detailed account of e-communication from an ICT perspective (BTRC, 2001) leaving the entire issue of e-communication vague and difficult to use Internet as an official communication medium.

E-Transactions

For legally valid e-transactions, not only authentication of electronic records is necessary, signatures of the parties to the online transactions are also required. The draft IT Act of Bangladesh contains provisions with regard to the legal recognition of electronic records and the usage of digital signatures (DSs) (§s 4, 5, 6). Where any law requires a signature on a document such requirement is fulfilled in the electronic environment by the use of a DS affixed in such manner as prescribed by the government (§ 6). It is worthwhile to note that mere usage of DSs in itself will not suffice the legal requirement. The affixing of DSs should be in a manner prescribed by the government. Thus, the government in accordance with the powers vested in it to make rules in respect of DSs (§ 11) may from time to time prescribe the manner in which DSs have to be affixed. For example, if the government at any particular time believes that computers are not secure enough devices to store and use DSs it may prescribe that only those DSs will be considered valid under § 6 which are embedded on smart cards

or other portable information storage devices. Furthermore, the Act allows electronic dealing with the government (§7) without creating any liability on the government to accept documents in electronic form (§10). §7 is titled as the "[u]se of electronic records and digital signatures in Government and its agencies". It states that electronic transactions with the Government can be "...effected by means of such an electronic form as may be prescribed by the Government". However, §7 with DSs in the title proscribes a liberal interpretation of the term 'electronic form'. This means that only DSs and its various forms can come under the terminology of electronic form and not other forms of electronic signatures (ESs). Thus, under the Act, PIN, password etc. cannot be prescribed by the Government as a form of ES for dealing electronically with the government.

Intellectual Property and Copyright

This is an important issue in relation to e-government. Bangladesh is a signatory of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and it has also been a member of the World Intellectual Property Organization (WIPO) in Geneva since 1985. However, Bangladesh has a poor record with respect to complying with intellectual property and copyright laws (IIPA, 2003).The legal provisions in this regard are laid down in §s 8 and 9 of the draft IT Act. The Act permits retention of documents in electronic forms provided there is no alteration to the original information (§8). Publications of rules, regulations and any other matter required by law to be published in an official gazette are also permitted under the Act to be published in an electronic gazette (§9). Although the Act does not cover every aspect of the copyright issue, an enactment of Software Copyright Bill in 2000 followed by a subsequent amendment of the Copyright Act 2000 incorporating issues related to ICT would help safeguard copyright and intellectual property (Islam, 2006). The Software Copyright Act extends protection to intellectual properties published in electronic media which is an essential ingredient of e-government (Karim, 2006).

Privacy and Security of confidential information

Security and privacy concerns have always been considered as an impediment to the use of ICT for online services such as e-government and e-commerce (Basu, 2004). E-government encourages transparency or openness in government system. While trying

to attain this goal, the risk of violating citizen's privacy comes up under scrutiny from ethical and legal perspectives. Raab (2004) questions the degree of openness of government or the regime of freedom of information while considering the privacy issue. He expresses his concerns about the use of public information for commercial use and other secondary uses without prior consent. E-Security is identified as one of the supply side barriers of e-government as security needs of government transactions cause technical difficulties and extra cost while implementing e-government. To secure government transactions, public key infrastructure (PKI) is designed and developed and to maintain security within government to government (G2G) communication, government secure intranet (GSI) has been developed (Margetts & Dunleavy, 2002). These e-security needs, linked with e-governance, are not covered by current administrative legal practices, which an IT Act could bring about in action. Patki et al. (2005) mention the increasing cases of e-security risks due to growing uses of e-governance applications in cyber cafes, Internet kiosks and community information centres.

Grönlund (2002) opines that citizen trust could only be established through providing adequate security, which needs technical systems like the use of DS. Legal security in e-governance could build citizen trust, as argued by Galindo (2002: 125), through 'creation of legal and arbitration mechanisms and procedures to permit enforceability of regulations'.

Presenting the weak trust scenario between citizen and government in developing countries, Bhatnagar (2004) also opines that a legal enabling environment could assist in improving the scenario. Therefore, it could be argued that all the associated legal challenges related to e-security might be addressed through an IT Act in e-government initiative so that citizens are confident about their data security through legal provisions and actions. The draft ICT act of Bangladesh aspires to deal with the different security related issues through number of provisions, which would be really meaningful through the enactment of the Act.

According to the draft IT Act, the originality of information communicated and accessed via internet need to be protected. The Act empowers the government to declare certain computer, computer system and computer networks as protected system (§ 75) while § 76 states that whosoever without authorization accesses the protected

system shall be punishable with an imprisonment up to ten years and/or fine up to Taka 200,000 (A$ 4,000). The purpose of these sections is to basically prevent confidential information residing on computers and computer systems of Certifying Authorities (CAs) and Controllers. However, according to a recent Internet security report "…threats with the potential to expose confidential information have continued to increase" (Symantec, 2005a). In such circumstances the punishment under § 76 seems inadequate.

The Act has also attempted to address security and trust issues. The Act empowers the government to prescribe appropriate security procedure (algorithm, codes, encryption etc) from time to time depending upon the prevailing commercial circumstances (§ 17). The Act states that where any security procedure has been applied to an electronic record the record shall be deemed to be a secure electronic record from the time of the application of the security procedure until its verification (§ 15). The security procedure can also be used with an agreement between the parties to create a secure DS (§ 16). Secure DS ensures that the DSs affixed are: unique to the person affixing it; capable of identifying the person affixing it; created in a manner or using a means under the sole control of the person affixing it and; is linked to the electronic record in such a manner that any change in the electronic record will invalidate the DS (Srivastava, 2005a). It is essential to mention here that § 15 is superfluous because an ordinary DS can fulfil what secure DS ensures.

§ 44 states that every subscriber shall take reasonable care with regard to his private key and ensure its security and confidentiality. What is meant by reasonable care? Who will be liable for the losses occurred due to the disclosure of the private key despite reasonable care taken by the subscriber? § 44 further states "…the subscriber shall be held liable for all the losses till he has informed the Certifying Authority that the private key has been compromised". In today's world where most of the computers, especially those in offices, are connected to the Internet or an Intranet and thus prone to online/external attacks the private key can be compromised in spite of the reasonable care taken by the subscriber (Srivastava, 2005b).

E-Crimes

It is needless to say, e-crime (often known as cyber crimes) is a global phenomenon and is engulfing the world at an alarming rate. Bangladesh is not immune from it[1]. Nonetheless, e-crime is a unique threat that can be carried out from anywhere against any computer system or user in the world. It is a global menace and is becoming increasingly difficult to control. As a result, governments, businesses and individuals all over the world are facing the new challenge of combating e-crimes (Serabian, 2000). A survey in the US shows that 85% of companies at least once experienced attacks on their networks and in 2003 alone, 22,000 attempts of unauthorised intrusion were made into the Pentagon network systems. According to another estimate, computer viruses annually cause $12b of losses for companies worldwide (Sabadash, 2004).

Bangladesh is yet to enact any cyber crime law. In its absence, it becomes difficult to make any e-authentication and e-certification and provide e-evidence against any e-crime. The draft IT Act contains civil penalties and criminal prosecution for unauthorised and unlawful activities related to the use of computer, computer system, etc. by any person. A person liable for unauthorized activities such as accessing; downloading; contaminating computer with viruses; disrupting a computer network and; denying access to any authorised person to his computer (§ 45) shall be liable to pay the person affected a compensation not exceeding taka 10,000,000 (A$ 200,678).

The Act defines hacking as:

> Whoever, with intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of "hacking" (§ 67).

The punishment for hacking is imprisonment up to three years and/or fine up to taka 200,000 (A$ 4,016) (§ 68), which is also the punishment for tampering with computer source documents (§ 66). The ever-increasing threat to Internet security and

[1] For example, on the 30th of October 2004 an anonymous email was sent to a leading national Daily in Bangladesh threatening to assassinate the country's leader of the opposition, while on another occasion, some hackers hacked the password of a government official internet service account in Bangladesh and made unauthorised access to internet using that account (Parveen, 2006).

where such threats are "…increasingly motivated by profit and desire to perpetrate criminal act (Symantec, 2005b) the punishment is very meagre.

Publishing of obscene information in electronic form is an offence punishable under the Act with an imprisonment of up to five years or/and fine up to taka 100,000 (A$ 2010) for the first offence, and imprisonment up to ten years and/or fine up to taka 200,000 (A$ 4016) for each subsequent offence (§ 69).

In situations where computer, computer system or computer network has been used for facilitating the commission of an offence under the Act but the offence itself has not been committed the person guilty shall be punishable "…for a term which may extend to half of the period of imprisonment prescribed for the offence or with fine or both" (§ 83).

The provisions of the Act are also applicable to offences or contraventions committed outside Bangladesh (§ 84) provided "…the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in Bangladesh". This is a very important provision for preventing offences under the Act which may involve a computer in Bangladesh for committing an offence outside Bangladesh. For example if a person uploads pornographic material from his computer in Bangladesh to a server in the US he or she may not be liable under § 69 alone but will be held liable if § 69 is read in conjunction with § 84.

Another important e-crime issue is identity theft. In the context of the increasing level of identity theft worldwide, it has become a necessity to undertake appropriate measures against this crime ("Australia nixes", 2005; Barker, 2002; Synovate, 2003; Hewitt, 2003). The draft IT Act, in this regard, contains some important provisions. § 77 of the Act states that a person making any misrepresentation or suppressing any fact from the CA or Controller for obtaining any licence or digital signature certificate (DSC) shall be punished with an imprisonment up to two years and/or fine up to Taka 100,000 (A$ 2010).

The Act also considers the liability of Internet service providers (ISPs) with respect to criminal activities. § 88 deals with Network Service Providers and states that no person shall be held liable for any offence/contravention for any third party information or data

made available by them if he/she can prove that the offence was committed without his knowledge or he had exercised due diligence to prevent the commission of such offence or contravention. This provision regarding ISPs are not appropriate as it creates a presumption that ISPs are at fault unless it can be proved otherwise. It may at times not be possible for the person to prove in evidence that he had no knowledge or he had exercised due diligence to prevent the commission of such offence or contravention. In this regard, the ISPs could also be held liable under the provisions of the Bangladesh Telecommunications Act 2001 for breaching their responsibility as network service providers (BTRC, 2001). Such a legal provision appears to be relatively harsh on ISP.

Although the draft IT Act is not without its criticisms[1], its enactment could have ushered in a new chapter in the IT history of Bangladesh. Unfortunately, it is yet to become a law and in the absence of a legally binding, comprehensive IT Act, Bangladesh needs to continue relying on existing traditional legal codes which are, by and large, unable to adequately address the unique and changing nature of e-crimes. The successful implementation of e-government will, therefore, remain as a difficult proposition.

Conclusion

E-government in developing countries is going through a process of transition. Bangladesh is no exception. The government of Bangladesh has declared the country's ICT sector as the 'trust sector' with a view to effectively use ICT in implementing e-government (BCS, 2006). However, despite such intention and apparent enthusiasm, the creation of a citizen-centric, transparent and efficient digital society based on e-government in Bangladesh still remains as a far cry. In the context of Gartner's typology of e-government, Bangladesh has got stuck in the second phase (interaction) of e-government process and has failed to demonstrate its ability to progress towards the higher phases of e-government, i.e., 'transaction' followed by 'transformation'. Given the increasing complexity and costs involved in moving towards the higher levels, a strong politico-administrative framework with the ability to frame and enforce law is considered as an important precondition to establish an ICT-driven government. In addition to providing legal recognition to important e-government functions such as e-communication and e-transactions, an effective legal framework is required to create an

[1] For a detailed criticism of the draft IT Act of Bangladesh, see Srivastava & As-Saber (in press).

environment conducive to promoting and executing e-government. It also offers safeguard to intellectual property and copyright of e-publications and helps identify, define and prevent the various e-criminal activities. Therefore, an appropriate legislations of an IT Act together with streamlining and linking other relevant legal codes are important in order to restrain and remedy crimes such as threats against property and individuals, piracy, hacking and fraudulent activities and illicit transfer and posting of data on the web (eg., viruses and pornographic materials),. In addition, specific legal authority needs to be exercised in order to protect intellectual property including copyrights. With respect to data security and interoperability, an appropriate legislation is required to be enacted to establish encryption standards and to accommodate international agreements on interoperability (MOSICT, 2002). It is, therefore, the time for Bangladesh to come forward and immediately enact the ICT Act to facilitate e-government and integrate itself to the global e-revolution.

References

Australia nixes ID cards. 2005, June 30. *p2pnet.net News*. Retrieved June 22, 2006, from http://www.p2pnet.net/story/5412.

Bangladesh Law Commission. (2002). *Final Report on the Law of Information Technology*. Retrieved June 10, 2006, from http://www.lawcommissionbangladesh.org/wplit.pdf

Barker, G. 2002, July 13. Stolen identity: The hidden cost. *The Age*. Retrieved June 22, 2006.

Basu, S. (2004). E-Government and developing countries: an overview. *International Review of Law Computers, 18*(1), pp. 109-132.

Baum, C., & A. D. Maio. 2000. *Gartner's four phases of e-government model*. Gartner Group Inc., Stamford.

BCS (Bangladesh Computer Samity). 2006. Industry profile and statistics: Bangladesh. Retrieved June 12, 2006, from http://www.asocio.org/resources/profiles/Bangladesh-Profile.pdf

Bhatnagar, S. 2004. *E-government: from vision to implementation: A practical guide with case studies*. New Delhi: Sage Publications.

BTRC (Bangladesh Telecommunication Regulatory Commission). 2001. *The Bangladesh Telecommunication Act 2001*. Dhaka: Bangladesh Telecommunication Regulatory Commission.

Burkert, H. 2004. The mechanics of public sector information. In G. Aichholzer & H. Burkert (Eds.), *Public Sector Information in the Digital Age: Between Markets, Public Management and Citizens' Rights*. Edward Elgar Publishing Limited, Cheltenham.

Cabinet okays draft of ICT act 2005. *The Daily Star*. 2005, February 15. Retrieved June 10, 2006, from http://www.thedailystar.net/2005/02/15/d50215061187

Caine, A. 2004. *E-government: Legal and administrative obstacles to sharing data held by Australian government agencies*. Canberra: Australian Government Information Management Office.

Dave, K. 2005. *Cyber laws for implementing e-governance initiatives and impediments therein*. Paper presented at the Conflux 2005: The e-Government Conference, October 17-19, New Delhi.

Galindo, F. 2002. E-government trust providers. In A. Grönlund (Ed.), *Electronic government: Design, applications and management*. Idea Group Publishing, Hershey/London.

Grönlund, A. 2002. Electronic government – Efficiency, service quality and democracy. In A. Grönlund (Ed.), *Electronic government: Design, applications and management*, Idea Group Publishing, Hershey/London.

Heeks, R. 2006. *Implementing and Managing eGovernment: An International Text*. Sage Publications Limited, London.

Hewitt, S. 2003, July 13. New fraud laws plan: Bid to protect identities. *Sunday Herald Sun*. Retrieved June 22, 2006.

IIPA (International Intellectual Property Alliance). 2003. Special 301 Report: Bangladesh. Retrieved June 20, 2006, from http://www.iipa.com/rbc/2003/2003SPEC301BANGLADESH.pdf

Islam, M. A. (2006, May 28). Bangladesh can now join ICT revolution. *The New Nation*. Retrieved June 19, 2006, from http://nation.ittefaq.com/artman/publish/article_28177.shtml

Jamil, I. 2002. Administrative culture in Bangladesh: Tensions between tradition and modernity. *International Review of Sociology, 12*(1), pp. 93-125.

Karim, H. N. 2006. IT industry take-off that never happened. Retrieved June 10, 2006, from http://www.bangla2000.com/Columns/Habibullah_N_Karim.shtm

Kubicek, H. (2004). Third-generation freedom of information in the context of e-government: The case of Bremen, Germany. In G. Aichholzer & H. Burkert (Eds.), *Public Sector Information in the Digital Age: Between Markets, Public Management and Citizens' Rights*. Edward Elgar Publishing Limited, Cheltenham.

Margetts, H., & P. Dunleavy. 2002. *Better public services through e-government: Academic article in support of better public services through e-government*. National Audit Office, London.

MOSICT (Ministry of Science and ICT). 2002. Information and communication technology (ICT) policy - 2002. Retrieved June 15, 2006, from http://www.bccbd.org/html/itpolicy.pdf

MOSICT (Ministry of Science and ICT). 2006. E-governance activities. Retrieved June10, 2006, from http://www.mosict.gov.bd/what_new.htm

Parveen, K. 2006, April 22. Computer based crime: A new legal challenge in Bangladesh. *The Daily Star*. Retrieved June 10, 2006, from http://www.thedailystar.net/law/2006/04/03/indepth.htm

Patki, T., S. Khurana, S. Sivasubramanian & A. B. Patki. 2005. *Product development for female cyber police programme*. Paper presented at the Conflux 2005: The e-Government Conference, October 17-19, New Delhi.

PCIP (Pacific Council on International Policy). 2002. *Roadmap for e-government in the developing world: 10 questions e-government leaders should ask themselves*. Pacific Council on International Policy, Los Angeles.

Raab, C. D. 2004. Privacy issues as limits to access. In G. Aichholzer & H. Burkert (Eds.), *Public Sector Information in the Digital Age: Between Markets, Public Management and Citizens' Rights*. Edward Elgar Publishing Limited, Cheltenham.

Robins, G., & J. Burn. 2001. Recreating government through effective knowledge management. In B. Schmid, K. Stanoevska-Slabeva, & V. Tschammer (Eds.), *Towards the E-society: E-Commerce, E-Business, and E-Government*. Kluwer Academic Publishers, London.

Sabadash, V. 2004, April 17. Victims of cyber crime. *Computer Crime Research Centre*. Retrieved June 15, 2006, from http://www.crime-research.org/news/17.04.2004/212/

Schartum, D. W. (2004). Information access legislation for the future? Possibilities according to a Norwegian experience. In G. Aichholzer & H. Burkert (Eds.), *Public Sector Information in the Digital Age: Between Markets, Public Management and Citizens' Rights*. Cheltenham: Edward Elgar Publishing Limited.

Serabian, J. A. Jr. 2000, February 23. Statement for the record before the Joint Economic Committee on Cyber Threats and the U.S. Economy, Washington D.C. *Central Intelligence Agency*. Retrieved June 17, 2006, from http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html

Srivastava, A. 2005a. Is Internet security a major issue with respect to the slow acceptance rate of digital signatures? *Computer Law & Security Report. 21, pp.* 392-404.

Srivastava, A. 2005b. Educating businesses about digital signatures. *International Journal of Business & Management Education*. Special Issue: Postgraduate Research in Innovative Methods of Teaching & Learning, pp. 1-16.

Srivastava, A., & S. As-Saber. in press. With time and patience the mulberry leaf becomes a silk gown: Regulating ICT in Bangladesh. *International Journal of Technology, Knowledge and Society*.

Symantec. 2005a, March 21. Symantec Internet security threat report highlights rise in threats to confidential information. Retrieved June 19, 2006, from http://www.symantec.com/press/2005/n050321.html

Symantec. 2005b, September 19. Symantec Internet security threat report identifies shift toward focused attacks on desktops. Retrieved June 19, 2006, from http://www.symantec.com/press/2005/n050919a.html

Synovate. 2003. *Federal Trade Commission - Identity Theft Survey Report*. Synovate, McLean VA.

Taifur, S., & M. Chowdhury 2003, June 30. *Problems of e-governance in Bangladesh and possible steps towards solution*. Paper presented at the Seminar on Road Map for ICT Development in Bangladesh, Dhaka.

Veysey, G. 2004. Intellectual property rights and domain names. In M. Chissick & J. Harrington (Eds.), *E-government: A Practical Guide to the Legal Issues*. Sweet & Maxwell Limited, London.

Epilogue:

The paper was prepared on the basis of information available until the 20th of September 2006. Subsequently, the parliament of Bangladesh passed the long-awaited ICT Act which was signed by the President of the Republic on the 8th of October 2006. However, the Act is yet to be available in the public domain and the pros and cons of this legal instrument remain to be seen.