

THE LEGAL ASPECTS OF ELECTRONIC GOVERNMENT IN PACIFIC ISLAND COUNTRIES: A REFLECTION^[*]

MOHAMMED L. AHMADU^[**]

INTRODUCTION

The main aim of the article is to examine the legal aspects of the structures which support the operations of e-governments and the extent of their adaptability to the circumstances of Pacific island countries. The article does not therefore intend to discuss the theories of governance or the ongoing debates on the pros and cons of good or effective governance in the region because they are outside the scope of this article.

The initiatives for regional cooperation and integration as envisaged in the Pacific Plan, particularly on the implementation of a regional digital strategy for enhancing information and communication technology will have direct bearing on the future development of e-government structures in the region. Furthermore, the wider strategic objective within the Plan of improving transparency in the governance, management and use of national and regional resources resonates with the idea of e-government acting as a facilitative tool to achieving that objective.

It is against this general setting that Part II discusses the general features of the legal regime supporting information and communication technology in some selected countries in the South Pacific. Part III examines the legal mechanics of Internet technology and how the architecture of the Internet may impact on electronic government structures. Part IV looks at the definition of e-government in relation to the some underlying theoretical issues. Part V examines the types of e-government structures. Part VI discusses the cost and benefit of e-government and Part VII concludes the article.

LEGAL REGIME OF ICT^[1]

The state of laws governing ICT in the region is as varied as the countries themselves. It is therefore impossible to provide one standard framework which appropriately reflects the circumstances of all island countries. However, a selection of the countries will give an indication of the current state of affairs and what may be needed in the future, especially in relation to the development and operation of e-government structures.

To begin with and by way of example, in all countries of the region, public procurement (which an important government activity) is still carried out through conventional contractual arrangements. At the moment no electronic version is contemplated except possibly in Vanuatu. To provide a fairly representative regional view of the prevailing situation, this segment will focus on Kiribati, Vanuatu, Tonga, Samoa and Fiji.^[2]

A. Kiribati

There is at present no national ICT policy in operation. In the area of intellectual property there is the *Copyright Ordinance*^[3] but this offers no recognisable protection for computer software or programs. The situation in Kiribati manifests an extreme case scenario in the South Pacific, possibly drawing countries like Tuvalu and Palau into its fold.

B. Tonga

The Kingdom has published a Communications Policy Statement in 2000. It has also embarked on policy

revisions in the area of ICT with a view to possibly including online economic activities. Other matters still under consideration include the civil service IT strategic plan, legislation on electronic signatures and authentication of network users' identities and international cooperation on security on cyberspace issues. It is also worthy of note that a new *Communications Act* was passed in 2000 and substantial amendments were made to the previous legislation covering radio, telegraph and broadcasting to take into account the use of digital broadcasting technology. Tonga has a national ICT consultative committee and the Tongan Telecommunications Corporation oversees the management of the country's DOMSAT.

C. Fiji

There is at present no comprehensive national ICT Policy. However, departmental level initiatives support a number of government information portals. There is a properly equipped and functional government ICT centre that services the IT needs of the government. The Southern Cross fibre-optics communications cable linking Fiji with the United States of America, Australia and New Zealand has been completed, allowing for high-speed data exchange and digital communications between these countries. The cabinet had in 2001 also discussed a paper on e-governance. There is a copyright law^[4] in existence and e-commerce and ICT-related laws are to be passed in the not distant future.

D. Samoa

There is no specific national ICT policy at present. However, through a number of initiatives, the government is able to support limited government information portals. An ICT steering committee was formed in 2002. A number of associated laws have been amended.^[5]

It is worth mentioning that Samoa in 1997 amended its *Communications Act* to encourage the operation and development of Internet services in the country by transferring to the Post Office, the property held by the defunct Pacific Internet Services Limited.^[6] Aside from this, there is nothing at present even in policy formulations to indicate a move in the direction of evolving a coherent national ICT policy.

E. Vanuatu

There is at present no integrated national ICT policy, but existing initiatives are adequate to support limited government portals (mainly for financial and commercial information). Importantly however, Vanuatu has passed two laws dealing with electronic commerce. These are the *Electronic Transactions Act 2000* and the *E-Business Act 2000*.

The *Electronic Transactions Act* is aimed at regulating the increasing pace of electronic transactions, which are in vogue today.^[7] This is primarily due to the emerging trends in the use of IT in the conduct of business dealings arising from the status of Vanuatu as an offshore centre. The law deals with the legal requirements of electronic records; communication of electronic records; electronic signatures; encryption and data protection; and intermediaries and e-commerce service providers. These emerging aspects of e-commerce are now regulated in Vanuatu.

The *E-Business Act* is aimed at complementing, in a general sense, the conduct of electronic business transactions. However, the scope of the law is limited to electronic businesses carried out by international companies.^[8] It is not of general assistance to all types of online contracts or transactions. The law covers cyber-suite contracts; electronic business contracts; cyber-suites and e-business accounts.

As earlier pointed out, the laws in Vanuatu are not part of a national IT or e-commerce policy strategy of the government. There is some progress. However, the current initiative is limited to private sector needs, which in any case have also been confined to the banking, Internet gambling and casino sectors of the economy.^[9] At least for now, there is no public sector support towards ensuring that a technological foundation emerges to complement the laws in this area. But the extent to which Vanuatu has recognised the need to pass these laws and is preparing to be integrated in the global information revolution, even if progressively indicates that the country is looking forward to developing the necessary integrated national infrastructure for e-commerce.

Given this scenario, it is clear that island countries still have a lot to do in terms of policy initiatives and investments if they are to establish the necessary infrastructure for the conduct of e-commerce and the conduct of e-government. Except for Vanuatu, where the legal framework has been established, Samoa, Fiji, Tonga, Kiribati and the others need very specific laws to deal with the various aspects of this new

phenomenon. The advantages of e-transactions are not restricted to the private sector. The public sector will have much to gain by engaging in it as well. For countries with limited resources, technological base and expertise, the benefits of e-government structures in administration and democracy cannot be underestimated. To realise these benefits, countries within the region have to inaugurate viable legal frameworks for electronic transactions.^[10]

LEGAL MECHANICS OF INTERNET TECHNOLOGY^[11]

Because e-government cannot effectively operate without the corresponding supporting technological structures, it is also important that a discussion on the relationship between the various mechanisms is examined. The primary vehicles for the development of effective e-government structures are digital technology and the Internet.^[12]

Internet technology provides the primary mechanism through which wide-spread electronic transactions can be conducted with relative push-button ease. The technology is particularly relevant to the situation of small island states of the South Pacific because of their remote geographical location, dispersed settlements and limited infrastructure. As will later be demonstrated, these constraints are not always necessarily disadvantages.^[13]

Other secondary issues relate to policy initiative and the reluctance by civil servants to embrace the benefits and opportunities created by e-government procedures for effective public administration. As observed in the e-Government Newsletter of Singapore:

The Internet presents the possibility of re-engineering government services to better serve the public. However, no matter how sophisticated our e-services are, it would defeat the purpose of providing these services if a large segment of our population is unable to access them. All government offices where appropriate, should also provide facilities for public access to e-services.^[14]

Electronic transactions, including the setting up of e-government structures and the use of the Internet^[15] to facilitate transactions illustrate a marriage of convenience between law and technology. While the medium or vehicle through which such transactions are conducted is provided by technology, the rules for validating and enforcing the transactions are supplied by the law. In this area, it is impossible for the law to exist independent of the technology and vice versa.

To this extent, a brief exposition of how the Internet works is useful in providing a rudimentary understanding of the operation of the system.

A. Internet Architecture

The Internet provides an open channel of electronic communication covering vast distances, using complex technology and equipment to transmit or exchange data, voice or video clips between multitudes of computers all connected in a global communications network system. In this regard, the Internet has appropriately been described as communications technology.^[16]

Information sent from one computer to another via the Internet is transported through several servers at random by using the most efficient route until it finally reaches its intended destination. The information is at the point of despatch broken into “packets” during transit, but reassembled into its original form at the point of receipt. For the information to be transported through the network, a protocol must be used the most important being the Transport Control Protocol (TCP).^[17] The Internet Protocol (IP) determines what server should receive the “packet of information” for onward transmission. To access the Internet via any website,^[18] the user must indicate the correct Uniform Resource Locator (URL) to visit.

To host a website would require the hosting agency to register a domain name. The use of this technological infrastructure means that at any given time, multiple copies of packets of information are temporarily copied by different servers in different locations worldwide. Of course, the physical location of each server depends on the routing. Emails are regulated by means of other application protocols, namely the Simple Mail Transfer Protocol (SMTP) and the Post Office Protocol (POP).^[19]

In dealing with the technological aspects of the Internet as a vehicle for online transactions, the legal

effects of the technology and operations involved need to be examined. Using with the Internet for purposes of online transactions would require the establishment of a domain name,^[20] especially from the point of view of the supplier of goods or services, whether in the public or private sector.

Generally speaking, the contents and ownership of the domain name may have nothing to do with the trademark protecting the domain name. The website and server hosting services are normally handled by an Internet Service Provider (ISP). Servers may crisscross different jurisdictions or transmit or exchange information passing through a number of converging or diverging legal systems. From a legal standpoint, the role of such intermediaries also needs to be taken into account. This is particularly so when the issue of client-server technology is brought into the picture. It is now possible for a user to obtain information indirectly from a third source- generally called re-user access.^[21]

Because Internet communication is conducted through computers and equipment, user identification becomes a problem.^[22] This requires a two-fold solution- namely legal and technical.

Technologically speaking, domain is the Internet name and address.^[23] The website forming the domain name may contain information whether copyrighted^[24] or not and may also have on it trademarks. The domain name may in some cases be a registered trade mark itself.^[25] Where this information is accessed and downloaded by different users at different locations, issues of copyright infringement are likely to be a source of legal concern.^[26]

As far as the informational contents of the domain are concerned, infringement of copyright or trade mark may be sustained if such written material enjoys copyright or trade-mark protection. While in normal situations exceptions to copyright may be justified, the position is not so settled in the case of Internet-based materials.^[27] There may also be the problem of determining the appropriate jurisdiction where the infringement took place and the proper law to apply. Where the domain name or address is non-country indicative, it is extremely difficult to determine the actual location of the breach.^[28]

In addition, servers or hosts that help transmit accessed or downloaded information from websites may themselves have to make several temporary copies of the packets of information in the course of transmission from one end of the network to the other. Cache or mirroring processes may in this regard equally raise the potential for some legal concern.^[29] In this instance, it is possible for the intermediary Internet service provider to be liable as a publisher.^[30] But again, unlike in traditional written materials, the act of the ISP in making copies or publishing information is an unconscious one because of the automated processes involved- necessitated by the advent of digital technology. In view of the fact that servers are programmed to take decisions without direct human involvement,^[31] the best way in which to avoid liability is to publish disclaimers on web-pages.^[32]

Given these developments, it is obvious that the architecture of the Internet will impact on the way e-government structures are to be conceived, established and managed. This brings to fore some challenges which touch on the legality of electronic evidence, automated decision-making and the appropriate forum for settling disputes created by these technological complexities. These are practical realities which the region needs to address.

DEFINITION OF E-GOVERNMENT

As it is with any phrase, “e-government” can be amenable to different definitions, depending primarily on one’s perspective or viewpoint. In general however, this paper defines it as a process of public administration and the provision of government services through the use of information and communication technology. This definition is wide enough to cover the use of facilities provided by the Internet, intranet and extranet communication systems.^[33]

The general idea behind such a wide definition is to ensure that the resultant e-government structures are in a position to facilitate effective public administration within national or local government sectors.

A. Theoretical Issues

In discussing the legal aspects of the structures supporting e-government, a number of theoretical underpinnings become immediately apparent: firstly, because of the nature of digital technology as a

facilitative medium,^[34] and secondly, because of the legal effects of the decisions reached in relation to the nature of the supporting electronic structures.

Without electronic systems, processes and decisions of governments are usually effected manually. However, the introduction of e-government will equally bring with it the need for decisions to be automated. Thus, the extent to which a merger of conventional and automated decision-making processes is to be established and in what specific areas of public administration are crucial to understanding the legal effects of e-government processes.^[35] This also raises another issue- the legal effect of the interface between manual and automated decisions.

The introduction of e-government will also significantly impact on the normal working environment. The conventional working environment (which usually is defined by physical space and interactions) will now be replaced by either a virtual working environment or a combination of the two. The extent to which public sector employees are or can adequately be prepared for this transition also needs to be carefully examined.

It is also obvious that because departments of governments are structurally different and perform different functions, the level of e-readiness might not be uniform across the various levels of staff and between departments. To that extent, interoperability or the interface of the different e-government systems within and outside the public sector creates additional legal and security dilemmas.^[36]

The establishment of e-government needs to also focus on the difficulty of clearly delineating the boundaries between the legal effects of automated as against those of the conventional executive and judicial decisions. A crucial question to ask is - where should the responsibility for such decisions lie. On machine or human or on both?

E-government structures help to facilitate meaningful civic dialogue and engagement between the public and government officials. This is healthy for effective governance and transparent administration. The need for this sort of engagement is no better needed than in island democracies with multiparty politics.^[37]

TYPES OF E-GOVERNMENT STRUCTURES

In this paper, there are four basic structures which e-government in the Pacific could take. These are: Information Portals; Legal Services Portal; Judicial Services Portal; and e-Voting Portal. Of course, the circumstances in individual countries might dictate what is or can be added to these initial e-structures.

A. Information Portal

This is by far the commonest e-government structure available. The rapid development of information and communications technology has brought with it the need for faster and easily accessible information on government functions and institutions in primarily two areas:

(a) Ministries, departments and statutory boards are generally expected to provide their email addresses and to also host websites detailing their functions and responsibilities. These sites could also act as information hubs on a wide variety of government services by providing information on investment opportunities, tourism potentials, health, and environment, to mention a few.^[38]

(b) Electronic filing of government documents, processing of on online permits, electronic tax payments and the submission of online public employment applications, to mention a few, will minimise wasting time on long queues and in getting mired in bureaucratic red-tape.^[39]

While the first portal is merely informational, the second is both informational and interactive allowing for valuable processes to be completed online, thus saving a lot of precious time. In general, portals cover the activities of the three arms of government, namely the executive, legislature and the judiciary.

B. Legal Services Portal

The provision of legal services to citizens should be distinguished from judicial functions performed by the courts. The emphasis here is on information, advice or materials that will improve access to justice. The recipient of such information, advice or materials will then be in a more informed position to process their rights. Three areas outline these e-government structures:

(a) Free-access online laws and regulations to help litigants who represent themselves in court or who may want to acquire a basic and rudimentary understanding of legal processes. This includes the provision of

wider public access to legal materials and advice in form of online legal aid and assistance.^[40]

(c) Electronic law reporting which covers statutes and judicial decisions made freely available to the general public.^[41]

(c) Online legal opinions to support the provision of legal aid and community legal service which may be automated, interactive or manually operated but processed online.^[42]

C. Judicial Services Portal

The role of the judiciary as a constitutional arm of the government and an independent and impartial arbiter of disputes forms the third organ of e-government. The role of the judiciary in upholding the rule of law, good governance and democracy cannot be over-emphasised be it in developed or developing countries. The importance of the role is more pronounced in island countries, which in addition to the demands of modernity are at the same time also expected to integrate and balance customary practices in their ways of life or even in some cases in the governance of their communities. For this reason, the role of e-government in relation to the judiciary is manifested in three main areas:

(a) Information and communication technology supporting systems for the recording of customary or formal court proceedings and filing of non-contentious court documents.^[43]

(b) The development and use of laws of procedure which support the admission of electronic evidence in civil and customary law claims and as a basis for settling such disputes.

(c) The use of automated electronic judicial decisions without human interface- a future possibility? ^[44]

D. E-Voting Portal

Another important aspect of e-government is an e-voting system. The conventional and manual voting system has its strengths and will for some time to come continue to hold sway. However, attendant problems associated with vote rigging, falsification of election results and general apathy towards the conventional voting system may in the long run help popularise the electronic alternative. An e-voting system is also not without its problems, particularly when viewed in the context of some countries in the region. However, it is worth mentioning that these problems are by no means only confined to either the South Pacific or to developing countries.

In the context of Pacific island countries, issues relating to digital access and digital divide between urban and rural settlements, problems of security of electronic votes and counting procedures and the security of e-voting systems in terms of authenticating signature and identity need to be addressed first.^[45] To establish the integrity of an e-voting system as an integral part of any e-government structure, it has been argued that it must in addition to all other safeguard and security measures also leave a paper trail.^[46] The cost and operational implications of this requirement will be enormous for countries with limited national budgets.

COST AND BENEFIT OF E-GOVERNMENT

An understanding of what is to be done to ensure that e-government is effective and meaningful to the lives of people also requires an analysis of the problems and prospects of the system. It is against this background that the following points are discussed.

A. Cost of Software and Equipment

The cost of software and equipment is fundamental and is one that will severely impact on the progressive development of e-government in the region. At the moment except for a few countries, the vast majority have no specific national ICT policies in place. To that extent, the creation of a knowledge-based and computer literate society does not represent an immediate priority for such governments. This trend needs to be reversed: by prioritising information and communication technology; the development of supportive legal framework; and the granting of appropriate incentives to the private sector to support electronic transactions both at the public and private sector levels.^[47]

B. Limited Bandwidth and Speed

While this is a problem, it is by no means confined only to Pacific island countries. Across the world, citizens generally suffer from this constraint which impedes the rapid download of data, voice or video transmissions. This also clogs the Internet highways and prolongs the time spent on accessing information on the Internet, thus negatively impacting on the availability of e-government services and products.

C. Access to Government Services

The establishment of appropriate e-government structures in the form of portals for online legal, judicial, corporate and voting services will go along way in improving the scope of access to government services. It will also speed up the utilisation of these services by the general public in view of the relative speed with which these can be processed. This is good not only for the economy but also helps in improving the quality of government services.

E-government structures have the capacity to improve the provision and delivery of government services. This will be a plus for democracy in that it can also promote good governance and transparency by linking public and private sectors online.^[48] The opportunities offered by the Internet need to therefore be fully tapped by the public sector in the region. According to Toland and Purcell:

South Pacific governments can use the Internet to assist with public sector operations. For example, ICT can provide governments with an increased capacity to collect revenue from fishing, agriculture and tourism. An intranet can allow different government departments to share information without having to make it available to the general public.^[49]

D. Opening up Rural Communities

The establishment of e-government will foster development opportunities in rural communities. It has been asserted that this will also promote civic engagement between public government officials.^[50] This is especially necessary in remote and rural communities which are far-removed from the main municipal and administrative centres of national governments. E-government structures will assist in bringing government services closer to the people thereby leading to effective governance because of transparency, greater and freer flow of public information.^[51] According to Chowdary, 'information and knowledge are what enable individuals to develop intellectually and economically.'^[52] The dispersed nature of island communities makes them ideal candidates to greatly benefit from the potentials of information and communication technology.

E. Attendant Risks

Continuous dependence on computers and related equipment and software may lead to associated physical and health risks. Although there is at present no evidence of this epistemological trend in any island country, it is time to begin considering appropriate policies and laws that will guard against that. The extent to which this may present significant occupational health problems in the region, only time will tell. However, it is still doubtful whether existing health, safety and occupational laws in the region can effectively deal with this new threat.^[53]

F. Technical Issues^[54]

These generally relate to security, data integrity and privacy. These issues are very crucial not only to the development, but also to the operations of e-government structures in the region. Because decisions governing various aspects of peoples lives are automated, the source and authority of decisions made online must be easily identifiable. This will be addressed in four ways:

(i) Security

The use of technology to transact online has brought with it the problem of user-identification.^[55] This is particularly so because of the remote nature of the transaction, the physical distance separating the parties and the ability to make instantaneous changes to electronic documents with little or no trace of detection. The cost-factor associated with putting in a place a reliable e-identification system will for some time to come make the technology suspect, at least from a legal point of view and particularly in the context of countries in the region. Perhaps a way forward for countries in the region is to set up a regional authentication agency which will integrate, optimise resources and save costs.

(ii) Signature Authentication

Flowing from the foregoing is also the problem of writing and authenticating digital signatures, which is equally very crucial to e-government operations.^[56] The use of private and public keys encoded in electronic documents to authenticate or validate electronic transactions is widely regarded as a means of safeguarding the integrity of online transactions and business deals. While encryption technology is also

aiding the process of authenticating digital signatures,^[57] appropriate laws will however be needed to support the transition from conventional to electronic signature systems.^[58] At present, almost all countries in the region are behind and need to catch-up by promulgating suitable laws to deal with issues pertaining to digital signatures; privacy of online public records and computer crimes, to mention a few.

(iii) Data Integrity

There are other problems associated with creating and managing 'round the clock' electronic databases, whether for public or private sector use.^[59] A fundamental issue here relates to data integrity. It is of utmost importance for the database to be accurate and up-to-date because it ^[60] helps to prevent fraud and unauthorised access or misuse.^[61]

Because e-government structures aggregate and process enormous amount of data and do so from different sources, the integrity of electronic records must therefore be of utmost consideration in the establishment and management of reliable online government systems and services.

(iv) Certification Authority

It is difficult for a single country to establish and manage a national certification authority^[62] to process digital signatures as a means of validating automated public decisions. There are financial and technical issues associated with the storage of digital signatures and the protection of such databases from viral and other attacks. For a certification authority to be a reliable manager of digital signatures, it must eliminate the major risks for using these signatures between the sender and recipient.^[63] Countries in the region need to put in place coherent national policies and legal frameworks to address the establishment and management of national digital certification agencies. In the alternative, stakeholders may consider establishing a regional certification facility to serve this need.

CONCLUSION

The future development of online government structures and services needs to perhaps take into account the setting up of subsidised solar-powered public Internet Kiosks for accessing data and for general public use. These can strategically be located in both rural and urban areas to facilitate access to information on government functions and public resources. The prohibitive cost of Internet access in the region is certainly not conducive to the long-term development and provision of effective online government services.

The level of enlightenment programmes on e-readiness is virtually nil in the region. The current curricula in schools need to be re-aligned to take into account the benefits as well the dangers of ICT. This campaign can also be instituted at different levels of the society and using a variety of media in order to prepare people to be part of new technologies. Sometimes unfounded resistance to new and emerging technology is likely to constitute the greatest obstacle to the future development of public online systems in the region more than any single factor.

The technology to be introduced must accord with each country's level of development. The systems must also be such that can be serviced and maintained locally as much as it is practicably possible. The use of appropriate technology in the design and operation of e-government structures will count as an important pre-requisite for the success of these systems in South Pacific island countries, and generally in other developing countries.

E-government is not and cannot be a complete replacement of the conventional system of public administration. It is to be seen more in the context of being a complementary approach to the existing government structures. This vision is to underline any national policy initiative which countries in the region are to adopt in pursuing their overall development strategies.

Lastly, the development and use of e-government structures is not without some practical challenges. However, the benefits for countries in the region will be far out-weigh the cost especially in this era of political and economic globalisation.

[*] A revised version of a paper presented at the Fifth IIDS International Conference on Governance and Development, December 1-4 2005, University of the South Pacific, Fiji.

[**] LLB (Hons), LLM (Lagos); LLM (Warwick) Ph.D. (USP); Associate Professor of Law, University of the South Pacific.

[1] This segment is partly based on: Mohammed L Ahmadu, "Overview of the Regulatory Framework for E-Commerce in Selected Pacific Island Countries" in *Harmonized Development of Legal and Regulatory Systems for E-commerce in Asia and the Pacific: Current Challenges and Capacity Building Needs*, Studies in Trade and Investment No. 54, UNESCAP Reference No: ST/ESCAP/2348 (28 December 2004). The laws and policies governing the regional ICT frameworks cited here were as at June 2002. See also, Mohammed L Ahmadu, "E-Procurement as a Development Imperative in Small Island States in the South Pacific" (2003) 10 *James Cook University Law Review* 51-70.

[2] The countries are drawn from Melanesia, Micronesia and Polynesia.

[3] Cap 16.

[4] *Copyright Act* 1999.

[5] These include: *Post and Telecommunications Internet Act* No 27 1997; *Postal and Telecommunications Act* 1999; and *Copyright Act* No 25 1998.

[6] See *Posts and Telecommunications Internet Act* No 27 1997; *Cf Communications (Amendment) Act* No 251 (2000) Niue. It amended the *Communications Act* 1989 by designating the ownership and management of the country's top level domain code, NU.

[7] This includes the practice of telemedicine.

[8] The domestic counterpart is the *Companies (E-Commerce Amendment) Act* No 27 2000 which amended s 378 of Cap 191. See also the *International Companies (E-Commerce Amendment) Act* 2000 which amended s. 10 of the *International Companies Act* No 32 1992.

[9] These are also offshore transactions.

[10] These may include, for example: (a) a Computer Misuse Act or Computer Crimes Act, or extensive amendment to the extant Penal or Crimes Act; (b) a Digital Signature Act or amendment to the *Evidence Act*; and (c) Digital Telecommunications or Multimedia or Telemedicine Acts, if and when appropriate.

[11] This segment is based on: Mohammed L Ahmadu, 'E-Procurement as a Development Imperative in Small Island States in the South Pacific' (2003) 10 *James Cook University Law Review* 51-70.

[12] The Internet was initially called: ARPAnet (Advanced Research Project Agency) (1969). It began as a military internet-work; then to an academic research internet-work; and is presently an open-commercial internet-work. This is today referred to as the: Internet.

[13] See generally, *Internet Infrastructure and e-Government in Pacific Island Countries: A Survey on the Development and Use of the Internet*, UNESCO (March 2002).

[14] See, 'E-Government Strategic Framework IDA Singapore' at <http://www.ida.gov.sg> (last visited 06 July 2006); and *The E-Government Handbook for Developing Countries* (2002).

[15] See, Andrew Terret and Iain Monaghan, 'The Internet- An Introduction for Lawyers' in Lilian Edwards and Charlotte Waelde (eds) *Law and Internet: A Framework for Electronic Commerce* (2nd ed, 2000) 1 who defines it as: "a public international networks of networks."

[16] See, Christopher Reed, *Internet Law: Text and Material* (2000) 10.

[17] See, R. Braden, 'Requirements for Internet Hosts- Communication Layers' in Christopher Reed, *op. cit* at 12 where he says: "The TCP controls the exchange of packets between hosts; it sets out the mechanisms for checking whether the packet has arrived, for checking to ensure that it has not been corrupted in transit , and for resending it if transmission fails."

[18] The protocol defining the content of information is the Hyper Text Transfer Protocol (HTTP).

[19] Christopher Reed, *op. cit.* 12.

[20] See, Daniel Tunkel and Stephen York, (eds) *E-Commerce: A Guide to the Law of Electronic Business* (2000) 20-22; For the UK perspective, see Markus Hoffman, 'Internet Domain Names- Legal Disputes and Challenges under UK Law' (2002) 13 *International Company and Commercial Law Review* 241-250.

[21] See, Christopher Reed, *op. cit.* 57; and Nick Page, 'Contracting Across the Internet' (1997) 20(9) *IP News* IF i-iv.

[22] Cf Raymond Perry, 'E- Conveyancing: Problems Ahead' (2003, May/June) *Conveyancer and Property Lawyer* 215- 224.

[23] See, Michael Chissick and Alistair Kelman, *Electronic Commerce: Law and Practice*, (2nd ed, 2000) xxxiii, where domain was defined as: "A part of the Internet name that specifies certain details about the host such as its location and whether it is part of a commercial, governmental, or educational entity. The address is written as a series of names separated by full stops"; See also Reed Christopher *supra* n.3 at 38; and William Black, "The Domain Name System" in Lilian Edwards and Charlotte Waelde, (eds) *op. cit.* 125.

[24] See generally, Hector L. MacQueen, 'Copyright in Cyberspace: Shetland Times v. Wills' (1998, May) *Journal of Business Law* 297-299.

[25] See, Charlotte Waelde, 'Trade Marks and Domain Names: There is a lot in a Name' in Lilian Edwards and Charlotte Waelde (eds) *op. cit.* 171; Susan Singleton and Simon Halberstam, *Business, the Internet and the Law* (1999) 13-49.

[26] Nick Page, 'Contracting Across the Internet' (1997) 20(9) *IP News* IF i-iv; and Yee Fen Lim, 'Copyright in the Digital Age' (April 2003) *The New Zealand Law Journal* 137; and generally, Paul Goldstein, *International Copyright* (2001).

[27] See generally, Fiona Macmillan, 'Striking the Copyright Balance in Digital Environment' (1999) 10(12) *International Company and Commercial Law Review* 350-358; and *British Horseracing Board Ltd & Others v. William Hill Organisation Ltd* [2001] R.P.C 621 CA). The contents of database are protected whether by copyright or not. No unauthorised extraction or reutilisation of all or significant portions of it are permitted.

[28] See, Stuart Dutson, 'The Internet, Conflict of Laws, International Litigation and Intellectual Property: The Implications of the International Scope of the Internet on Intellectual Property Infringements' (1997, Nov) *Journal of Business Law* 495-513.

[29] This allows the attaching of special programs such as Java and Active-X to process the making of copies of web pages. See generally, Christopher Reed *op. cit.* 19 and 24.

[30] See generally, Mathew Collins, *The Law of Defamation and the Internet* (2001).

[31] *Ibid* at 79.

[32] Cf John Prebble et al, 'Databases by Jurisdiction' (2003, Nov) *The New Zealand Law Journal* 125.

[33] See also, Westcott, 2001, ADB who defined it as: the interaction between government and its employees, business and citizens over the Internet; and *The South Pacific ICT Situation-Online Government Survey 2000*, UNESCO & COMNET-IT.

[34] Digital technology- is defined as: a device or method that uses discrete variations in voltage,

frequency, amplitude, location etc to encode, process or carry binary (zero or one) signals for sounds, video, computer data or other information. (ASEAN Secretariat).

[35] For a technical and scientific analysis of manual and automated interface processes, see generally, Umesh Shankar & Reiner Sailer, 'Toward Automated Information Flow Integrity Verification for Security-Critical Applications' at <http://http://www.cs.berkeley.edu/~ushankar/research/cwlite/cwlite.pdf> (last visited 06 July 2006).

[36] On the different levels of automation necessary to achieve some degree of interface with manual systems, see generally, M. L Cummings & S. Bruni, 'Collaborative Human-Computer Interface in Network Centric Warfare' at http://web.mit.edu/aeroastro/http://www/labs/halab/papers/Cummings_TTCP.pdf (last visited 06 July 2006); and on the non-civilian application of such interface decision-making processes, see generally, Thomas Russ & Andre Valante, 'Capturing Assumptions Underlying Planning Decisions' at <http://http://www.isi.edu/isd/JFACC/SDA/SDA-interface.html> (last visited 06 July 2006).

[37] See generally, InfoDev-World Bank & Centre for Democracy and Technology, November 2002.

[38] The various government portals on the web illustrate this scenario.

[39] See for instance, *Internet Permit Web User Guide* at http://http://www.sjgov.org/commdev/cgi-bin/cdyn.exe/handouts-building_web_user_guide?grp=handouts-building&obj=web_user_guide (last visited 06 July 2006).

[40] John Zeleznikow, 'Using Web-based Legal Decision Support Systems to Improve Access to Justice' 11 (1) 2002 *Information & Communication Technology Law*.

[41] See for example, <http://www.paclii.org>; <http://www.worldlii.org>; <http://www.auslii.org>.

[42] Future Pilot trial- USP Community Legal Centre.

[43] Such as simple ex parte applications and consent orders.

[44] Cf Jack G. Conrad & Daniel P. Dabney, 'Automatic recognition of distinguishing negative indirect history language in judicial opinions' at <http://portal.acm.org/toc.cfm?id=502585&type=proceeding&coll=GUIDE&dl=GUIDE&CFID=61301995&CFTOKEN=69299212#502632> (last visited 06 July 2006). See also *Garton v Hunter* [1969] 1 All ER 451.

[45] Cf the perspective of more advanced economies. See generally, T, Adayoshi et al; 'Analysis of Electronic System' (July 2003) *John Hopkins University Information Security Institute Technical Report TR 19*.

[46] See generally, Kim Zetter, "E-Votes Must Leave a Paper Trail" at <http://http://www.wired.com/news/evote/0,2645,61334,00.html> (last visited 06 July 2006).

[47] Cf with the case of Malaysia where the National Information Technology Agenda of 1996 set the momentum for e-commerce, the development of appropriate hardware and software technologies and the institution of a legal framework to accommodate any accompanying changes. A significant aspect of this policy was the creation of the Multimedia Super Corridor aimed at fostering the development of e-commerce. Similar measures were taken by Singapore. This started in 1996 with the Electronic Commerce Hotbed Programme- a national policy initiative aimed at facilitating e-commerce in the country. In 1998, the country moved another step forward by inaugurating the Electronic Commerce Master Plan. See generally, P. S. Sangal, 'Malaysia Creates Legal Infrastructure for its Multimedia Super Corridor' (1997)12 *International Company and Comparative Law Review* 428-430.

[48] See generally, *UNESCO Report*, March 2002.

[49] See, Janet Toland and Fuatai Purcell, 'Information and Communication Technology in the South Pacific: Shrinking the Barriers of Distance,' December 2002 *Development Bulletin* 91.

[50] See, *InfoDev-World Bank & Centre for Democracy and Technology*, November 2002.

[51] Cf Nasser Saidi et al, 'e-government: Technology for Good Governance, Development and Democracy in the MENA Countries' at <http://www.ictdar.org> (last visited 06 July 2006).

[52] T. H. Chowdary, 'Policy and Regulation to Bridge the Digital Divide' at <http://www.inomy.com> (last visited 06 July 2006).

[53] See for instance, Health and Safety at Work Act 1996 (Fiji); Health and Safety at Work Act Cap 195 (Vanuatu); or Occupational Health and Safety Act 2002 (Samoa).

[54] Partly an adaptation from: Mohammed L. Ahmadu, "Legal Aspects of Electronic Land Registries in South Pacific Island Countries" Real Property Law Teachers' Conference, 1-3 July 2004, University of Canterbury, Christchurch, New Zealand.

[55] Perry, above n 22, 215-224.

[56] Digital signature is defined as an output of algorithm using computing process. See Adrian McCullagh et al, 'Cryptography: From Information to Intelligent Garbage with Ease' in Anne Fitzgerald et al (eds), *Going Digital 2000: Legal Issues for E-Commerce, Software and the Internet* 207 (2nd ed., 2002); and Stephen Mason, 'Practical Problems of Digital Signatures' (2003, Nov/Dec) *I. N. L.* 9-10.

[57] Cf Stephen Mason and Nicholas Bohm, 'The Signature in Electronic Conveyancing: An Unresolved Issue' (Nov/Dec. 2003) *Conv. & Prop. L.* 460-472; Deveral Capps, 'Conveyancing in the 21st Century: An Outline of Electronic Conveyancing and Electronic Signatures' (2002, Sept/Oct) *Conv. & Prop. L.* 443-455; and Phillip H Kenny, 'Are Electronic Signatures Safe or Not?' (2002, Mar/Apr) *Conv. & Prop. L.* 94-96.

[58] Cf *Electronic Signature in Global and National Commerce Act* (USA); *UNCITRAL Model Law on Electronic Commerce* 1996; *Singapore Evidence Act* (1996) s.35; and the *Canada Uniform Electronic Evidence Act*.

[59] Lesley Pollock, 'E- Conveyancing: Is It Going To Work?' (2002) 4(2) *Elec. Bus. L.* 16.

[60] See, Graham Norwood, 'Cobwebs Shaken Off Conveyancing' (2001) (0128) *Estates Gazette* 126-127.

[61] Mark Heighton, 'Electronic Conveyancing: Moving With the Times' (2002) 3(12) *Elec. Bus. L.* 11-12; Phillip H Kenny, 'Digital Fears' (2002, Jan/Feb) *Conv. & Prop. L.* 4-6.

[62] A certificating authority is the issuer and manager of approved digital signatures. It is a verification system for all its issued signatures, hence guaranteeing the authenticity of signatures used in electronic transactions.

[63] Stephen Mason, 'Practical Problems of Digital Signatures' (2003, Nov/Dec) *I. N. L.* 9-10.