Rapporteur's Report

Sixth National Cyber Security Conference

Mona ICT Policy Centre, CARIMAC, University of the West Indies, Mona

November 27-28, 2018

Introduction

The 6th National Cyber Security Conference, hosted by the Mona ICT Policy Centre, CARIMAC, UWI, was convened at the UWI Regional Headquarters November 27-28, 2018. The theme was **Data Protection: Security Big Data, Understanding Biometrics and Protecting National ID Systems.** The event consisted of an Opening Ceremony and five plenary panel sessions over the two days. Lead organizer and Conference Chair was Professor Hopeton Dunn, with partnership from the Internet Society (ISOC), International Telecommunications Union (ITU), and the Canadian High Commission in Jamaica. Sponsors were National Commercial Bank NCB (Lead Sponsor), Henlin Gibson Henlin, Spanish Court Hotel and the RJR Communications Group.

Over 180 registered participants attended the conference each day.

A pre-conference reception for presenters, chairs and sponsors was hosted on November 26, 2018, by the Canadian High Commission.

Day 1 – Tuesday November 27, 2018

OPENING CEREMONY

In delivering the Chairman's Opening Remarks, Professor Hopeton Dunn welcomed all attendees, and in particular, the Minister of National Security, Dr Horace Chang, who was Guest Speaker. He also extended special welcome Lead Presenters visiting from overseas, the representative of ISOC, Mr Shernon Osepa, Dr Gunjan Mansingh representing of Campus Principal, NCB's Senior General Manager, Mr Brian Boothe and to the Political Ombudsman, Mrs Donna Parchment Brown.

Consistent with previous Conference outcomes, Prof Dunn renewed the call on the Parliament to ensure passage of the long overdue Data Protection Act of Jamaica especially at a time when we contemplate the collection of high volumes of personal biometric data with a proposed establishment of the National Identification System (NIDS).

This conference is also being convened at a time when threats, risks and challenges on the internet are proliferating, and when governments and companies are placing many of our critical national assets online, making us vulnerable as a country and as individuals.

Prof Dunn also voiced the expectation that universities will take the lead to develop the skills to combat cybercrimes in the region and to shape the internet by using our own personnel from the region.

Guest Speaker – The Honourable Dr Horace Chang, MP:

Technology has significantly increased the amount of data available in cyberspace. The Internet of Things (IoT) and the advent of big data analytics have enabled major advancements in the daily operations by utilizing available data, particularly in crime fighting efforts.

With the rapid advance in technology and the amount of data available in cyberspace, the government of Jamaica is moving to ensure that the Data Protection legislation is available shortly to combat cybercrime and protect sensitive data. Such a measure will facilitate the operation of NIDS and impact the storage of personal data.

The Major Organised Crime and Anti-Corruption Agency (MOCA) as one of the country's key security organizations, will carry a lot of this burden. We will have individuals trained in cybercrime, individuals who can patrol the dark web and look out for risk and challenges in order to take steps to mitigate and correct these challenges.

The government is committed to safeguarding the information entrusted to us and utilize it in the most efficient and effective manner. We will continue our co-operation with public and private stakeholders to advance our technological and security infrastructure.

Appreciation was extended to the UWI and in particular to the Mona ICT Policy Centre at CARIMAC for so successfully hosting this event for the 6th year running.

Her Excellency, Mrs Laurie Peters, High Commissioner of Canada:

CARIMAC must be congratulated for hosting the 6th National Cyber Security Conference, and the High Commission is pleased to collaborate with the University of the West Indies again this year to bring this event which allows us all to engage on this issue of national and international importance.

There is definitely high awareness, interest and momentum here in Jamaica. There were several activities last month related to cyber security as part of the International cyber security awareness month. For example, Jamaica's Cyber Incident Response Team partnered with the JCF and others to increase awareness amongst consumers, students and businesses. Jamaica is proving to be a good example of leadership as strategies and policies fall in place or almost in place such as the national cyber security strategy that has helped to make Jamaica what I understand to be the best prepared countries in the Caribbean on this front.

Canada is a key international partner with Jamaica especially when it comes to our efforts to fight crime and violence. Jamaica has benefitted from Canadian support through our Anti-Crime Capacity Building Programme as well as our Counter-Terrorism Capacity Building Programme. Through these forms of support, we've been able to provide training. Just last week our financial crime investigators from the Royal Canadian Mounted Police delivered an anti-money laundering course to a variety of law enforcement agencies and prosecutors here in Jamaica. The growing use of virtual currencies presents a unique challenge to financial regulatory bodies. Canada is offering training in this area to help Jamaica stay ahead of that curve.

Canada has taken some of the following steps to improve its cyber security:

- In 2010 a Cyber Security Strategy was implemented for government systems
- Legislation has been introduced to keep pace with the digital economy and growing cyber threats to citizens and businesses. Some examples are the Anti-Spam Act, the Electronic Commerce Protection Regulations and Secure Electronic Signature Regulations.

Address by NCB Senior General Manager, Mr Brian Boothe:

Today, in this digital era, privacy and security encompass both personal and digital spaces. No longer are the two separate issues. Instead, one directly affects the other and that is why they form a significant part of our public discourse.

This annual conference has become pivotal as it addresses, this year the theme: Data Protection— Securing Big Data, Understanding Biometrics and Protecting National ID Systems.

Data protection deals with the ability of organizations and individuals to determine what data in a computer system may be shared with third parties.

Locally, the conversation about data privacy has been in the public sphere largely due to the proposed passage of the NIDS.

Globally, the issue of data privacy from a legislative standpoint seems to be moving at a slow pace. So far, 57% of countries have data privacy laws, another 10% have begun the process, 21% have no legislation while there is no data for the remaining 12% of countries. In the case of Jamaica, we have taken steps to ensure data privacy. We have laws governing transactions, cybercrimes and consumer protection. However, the necessary legislation to govern data protection and privacy are still in the draft stages.

Mr Shernon Osepa of ISOC reaffirmed the support of his organization for the annual conference and was pleased to assist in providing lead presenters, including for this year's event. He reaffirmed the critical importance of the Conference theme and commended, MICT and in particular, the Conference Chair, for leading this important component of a national and regional dialogue on cyber security.

Dr Gunjan Mansingh, representing Campus Principal Professor Dale Webber, brought greetings and commendations from UWI to the Conference organizers and attendees. She

outlined several global and regional developments affecting cyber security and the continued role of the UWI in helping to prepare Caribbean society to cope with the threats.

SESSION ONE: Data Protection: Issues and approaches

Jeff Wilbur:

The conference addressed the emerging trends in cyber-protection regulations. These trends were primarily prompted by the General Data Protection Regulation (GDPR) of the EU taking effect. As a key part of overcoming the challenges we face with transitioning to cloud, we must understand security posture of partners. This simply means making the transition more contractual. Utilize third parties to verify/ monitor transition as well as being mindful of critical data. It was suggested that we employ multi-factor authentication such as Biometrics as a way of overcoming the challenges we will face with threats such as those caused by users as risk and the gateways. (see PPT Report)

Damian Donaldson:

Data owners are those who access and use the organization's data. We should develop policies around those who accesses the data and how it is accessed.

In the course of data protection, data owners are the ones to whom the data "belongs". They determine how their data are to be used, accessed and protected (e.g. business units, citizens via govt. etc.) It was suggested that data loss prevention systems can be monitored and can block the movement of sensitive data via email, web, usb etc. Enforcing data protection compliance with regulations can be difficult. Current data encryption tools do not protect data in use and need higher levels user involvement. (see presentation)

Nicole Foga:

Under the new charter of rights, there is an untested constitutional right to privacy. As such, there is no right recognized in Jamaica to data protection. Some challenges may be identified, such as rising administrative costs, hiring specialists and consultants, updating employees training and conducting audits.

The speaker emphasized the need for vigilance with National compliance standards as well as international standards including GDPR which came into effect for the European Union May 25th 2018, with implications for global partners.

With the GDPR EU and European Economic Area (EEA) citizens now have greater control over their personal data and assurances that their information will be securely protected across Europe. Its application is not restricted to companies selling and storing personal information about citizens in Europe, but includes partners around the world.

According to the European Union Data Protection Act 2017, as it relates to sensitive data: Any offence by the data subject or any proceedings for any offence committed or alleged to have been committed by the subject, the disposal of such proceedings/ the sentence of any court in such proceedings will be determined by the EU Commission. Therefore, processing becomes necessary for the exercise of any function of the government/minister/department.

According to Data Protection Act 2017: Sensitive data relates to those collected for medical purposes, undertaken by a health professional or a person under a duty of confidentiality equivalent to a health professional.

Data controllers' compliance requirements as it relates to registration: No entry shall be retained in the register for longer than 6 months except on payment of the prescribed fee.

QUESTIONS AND ANSWERS

Question (Audience): Given that globalization is bringing Caribbean states geo-politically closer to developed nations such as United States and European Union, this closeness is being brought about through the sharing of technology and most recently the development of cloud technology. How much more difficult has it become for Caribbean governments to protect themselves from cyber-attacks such as data terrorism?

Response (D. Donaldson): It is established that there are significant challenges from cyber-attacks. The difference though is the lower level of maturity within the Caribbean as opposed to North America. We may be perceived as a softer target, a more vulnerable target because we are not as mature in terms of our security thinking and practices. From that standpoint, we know that economically, countries in the Caribbean face challenges

generally. When you consider the whole issue of cyber security and data protection, there is no way to escape the fact that you're going to have to put money into it.
The Minister (of National Security) mentioned earlier that it is an expensive affair, so economically governments in the Caribbean have traditionally faced challenges as far as implementing the necessary policies and strategies. They are going to be required to comply with these new international regulations and to position themselves more advantageously in the global market.

Question (Audience): If you are doing business with other Caribbean countries but one doesn't have data protection legislation in place and you are also doing business within the country with another company and that company is not being prudent with your data, what are the means to address both situations and what is the reporting procedure? Is there any means of compensation if your data is lost?

Response (N. Foga): In Jamaica we have not yet passed the draft Data Protection Act. but practically, a number of overseas and local companies operating in Jamaica, for example, the business process outsourcing sector, they do compliance contractually. They put down the standards you must comply with; they do train and if you are in breach, it is probably a breach of contract: they can sue or be sued. Part of the problem we have had in Jamaica and other countries is with persons who are in jurisdictions where they have strong data protection legislation, who have been hesitant to go into areas where there is no legal framework and the 'work-around' for this has been through contract terms and conditions.

Response (D. Donaldson): From a business standpoint, if you're going to be outsourcing aspects of your operations you still need to have the assurance that whoever you're partnering with is capable of protecting your data at the levels to which you require. One of the tools which exist in order to provide you with that assurance are audit certifications such as SSAE 16 & SSAE 18 (SSAE – Statement on Standards for American Engagements). It states that third parties have a system of internal controls that is adequate for protecting the data that you're going to give them. They do annual audits

that test the controls counterparts have and see whether they are performing adequately. After it is made, you as the person entering into business with them can request and demand from those who do that. If they do not however have certifications, the trading partner try to encourage them strongly that they need to go through a similar process with independent assurance that they are actually doing what it is they are supposed to do.

SESSION TWO: Protecting Big Data/ Protecting Rights

David Green:

Acknowledged that his domain was more in marketing than engineering or Technology. However, the messaging around national data protection is a crucial part of the mix. Data is the new gold, it is the new oil. It has to be protected. If it is not protected someone else will take it.

According to National Institute of Standards and Technology (NIST) *Intro to Privacy Engineering & Risk Management in Federal System:* Protecting privacy is often said to require a multidisciplinary approach including law, sociology, information security, ethics and economics. (SEE PPT REPORT)

Stephanie Williams:

As it relates to storing personal data: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

It should be stored lawfully, fairly and transparently.

According to the right of access: Individuals can request information verbally or in writing.

You must provide information without delay and within the timeline stipulated.

If the request is made electronically, you should provide the information in an accessible electronic format.

Sean Thorpe:

Important Biometric identifiers such as the duplication feature is not available in other identification systems.

Biometrics can provide significant advantages toward becoming a digital society. (see PPT)

QUESTIONS AND ANSWERS

Question (audience): What advice would you give us to look out for legitimate sources such as identification authentication controls?

Response (J. Wilbur): Email authentication allows the recipient of the email to verify that it is really from who they say it's from. That is in place for all the big consumer mail boxes such as Gmail and Microsoft. This can help determine whether the email is a fraud.

Question (audience): Can we afford the provisions under the GDPR and is this a one size fits all or is there room for adaptation?

Response (D. Green): Yes, there is room for adaption, but it comes onto the matter of cost and the issue of cost. Cost could be prohibitive for many institutions trying to become compliant where GDPR (General Data Protection Regulation). There is a resource cost involved. The GDPR regulations calls for you to hire someone known as the data protection officer and this person is actually responsible for ensuring that the regulations are in fact implemented inside the organization and that the regulations are in fact complied with. It is not a one size fits all.

SESSION THREE: Technologies of Data Management and Protection- Biometrics

Curtis Busby-Earle:

Biometrics is a unique physical attribute. Fingerprints are the most classic biometric, with face, iris, voice, hand geometry and other systems in use and more in development.

The emphasis is placed on personal identification and authentication for delivery of services. Other ways and means of securing data such as cryptography are widely used and have been proven to provide required levels for strong protection. (See PPT)

SSP Carl Berry:

Shared experiences of the Jamaica Constabulary Force in crimes relating to human trafficking as well as other types of criminal activities. Some online challenges with online platforms include**:**

- Cyber extortion
- Cyber bullying
- Identity theft

According to the Defence Advanced Research Projects Agency: While we focus the vast majority of our security efforts on protecting computers and networks, more than 80% of cyber-attacks and over 20% of those from nation states are initiated by exploiting humans rather than computer/ network security flaws.

QUESTIONS AND ANSWERS

Question (audience): What methods or strategies are you aware of that can protect these biometric systems that utilize encryption propagated or operated through computer memory? Why wait until it is decrypted at the time of use? And how can you protect against that vulnerability?

Response (C. Busby-Earle): To actually use biometrics it must be decrypted. There are ways that you can encrypt data on a file that still does not change the fact that within memory, and specifically within RAM that given a hacker or someone who is determined enough, can actually still access that data because it must still be decrypted in order to be used. But once it is memory resident then it is actually vulnerable.

Day 2 of the Conference was concluded by summary remarks by Conference Chair Professor Hopeton Dunn

Day 2 – Wednesday November 28, 2018

SESSION FOUR: Protecting Against Cyber Threats to National Assets

Preliminary comments by Mr. Carlton Samuels:

It was reaffirmed that Data is the new oil. It is the centre of the data economy. The most valuable companies these days are data companies. In the national space, banks have data for various reasons. Other data include election data and health data. Telecoms companies also hold a lot of data. Government entities hold data across the board. Data is valuable.

Where there is value someone will always try to exploit it. Whether its electoral lists, public accounts, power supply systems, public power grid data - a lot of the controls are automated. Its machine to machine communication that keeps it going. It's important to safeguard that data.
Apology tendered for absence of speakers from Electoral Office and Office of Disaster Preparedness (ODPEM). Representative from health sector, UWI Hospital was welcomed.

Kevin Allen:

The University Hospital of the West Indies Hospital has been challenged to update the operations of the hospital to be more efficient. Storage, security and how data is managed are important. We are patient and physician centric.

We have a growing team of technology savvy clinical and administrative employees. We are also growing the ICT team. The Ministry of Finance was approached to secure funding. 25 ICT posts are being advertised to improve and manage infrastructure and data being collected. 10 application systems are being run at the UWI Hospital. Protective mechanisms and controls are in place. How persons access data is an issue. We are a teaching hospital. This can pose a challenge.

In the Departments dealing with HIV or Psychiatry, systems are open to clinicians but it is also open to surgeons who don't necessarily need access to all data. How do we control family and next of kin that access the information? We have to deal with these subtle issues.

Theft of computers, phishing and other issues have to be dealt with. How do we respond internally? We are developing policies. We have approval for a policy division which will draft, implement and monitor the risks to ensure they are minimized. Then we have the physical security. The physical device should not leave the hospital. We need strong robust security networks.

One area is education and training. There must be continuous training and development. The industry is not static, so training will keep us ahead of the curve.
Acceptable use, password policies – these are important for our staff. We advise them on what best to do.

Discussion of surveillance and privacy of patients is currently being considered. We are looking at whether there will be breaches of the patient's privacy. Doctors can stay at home and look at their smartphones and prescribe medication remotely. But if the family members see that information how do we deal with that breach?

We are experimenting with telemedicine in deep rural Jamaica. How do we secure data given to clinicians in rural Jamaica? Radio frequency identification is used to protect data- that's one mechanism. The system is always evolving.

We are working with the risk management team to manage the data. We hope to derive an efficient service that Jamaica and the region can be proud of. That medical students can have information at the tip of their fingers. Collecting the research can help us in delivery of our services.

QUESTIONS AND ANSWERS

Question (Professor Dunn): How are our critical assets being saved and stored? We want to be satisfied that the custodial role over health data being carried out is effective. Electoral systems, banking, telecoms, hospital and health services are all online. There are other elements that can leak data and create risks. Safe custody of patient data – how

far along is UWI Hospital in digitizing and safeguarding patient data and allowing for inter-hospital data exchange?

Response (K. Allen): We have 20,000 plus records now online. 30%. Patients now coming in, we take their info. We also integrate their info with insurance companies. We have not communicated with rural hospitals. 3 weeks ago, Minister of Health unveiled this plan. UWI Hospital is taking the approach seriously. However, we are hampered by capital constraints. We now have young managers coming through to run the hospital. We have seen an increase in the inflow. We have also commenced a UWI tech centre to make further investment. We are partnering with Advanced Integrated Systems to help us manage the data. The government is monitoring the progress and functionality.

Question (L. Haughton - audience): Has an ICT audit been done and will it be made public?

Response (K. Allen): No audit has been done. We are still in the implementation phase. It will not be made public once completed. It's for management's purpose.

Question (audience): What would happen if a data breach happens?

Response (K. Allen): There are tight controls in the system if a breach occurs. I do agree the audit should be done, but be we are monitoring the system as it is being rolled out. We would need an independent review of what is happening.

Question (D. Donaldson – audience): Many of the legacy systems were not designed with security in mind. Physical security on hospital premises is also a serious issue. Paper records are still out there. How do you plan to deal with the physical safety of devices and paper sources?

Response (K. Allen): We are working with international partners to improve our current systems. The tech company Advanced Integrated Systems Ltd stores our data at an

undisclosed Caribbean location, and in another secondary storage area outside the hurricane belt. Once somebody is trained it is difficult to keep them. C. Nicholson (UWI Hospital) – We are working through the processes and with our internal team and external developers. We are putting the necessary steps in place.

Question (Professor Dunn): How far are we in equipping emergency response vehicles such as ambulances with safety devices?

Response (K. Allen): We are not very equipped. We are trying to secure dockets. But we are digitizing as we go along. Ergotron is a partner we have identified to equip our data. It is a costly exercise.

Question (audience): Has the hospital contemplated using the cloud for data storage?

Response (K. Allen): We have a limited talent pool available to us, so we have external partners to help us manage this process. We need to improve our outsourcing.

Question (audience): How do we ensure data is safe when stored in foreign jurisdictions?

Response (K. Allen): These issues are built into contracts. They sign confidentiality clauses.

Question (D. Donaldson – audience): From a critical infrastructure standpoint, where are the regulators in terms of setting standards for the involvement of third parties and the movement of data outside our jurisdiction? How much of a say have they had in making these decisions?

Response (C. Samuels): The legal framework does not exist for that sort of issue. The OUR can intervene on a general requirement. But the draft Data Protection law has a role to play. The Data Protection law is important to create regulations across the board.

Financial institutions and banks are subject to heightened legislation, but even that is not up to date. There is need for an all-encompassing legislation for the regulator to have oversight. Employee integrity is an issue. There is a requirement for background checks on employees. The persons working in ICT are potentially very dangerous.

Question (Professor Dunn): Many of the critical assets that used to be stored in the public sector have now been divested to the private sector. The electoral office had some ideas about 10 years ago to market the electoral list, and it caused an issue. How are the threats of breaches and misuse of public data being treated now?

Comments (C. Samuels): The government's Cyber Incident Response Team (CIRT) has been created to codify what happens if there is a data breach. It's a national team for both the private and public sector in Jamaica. eGov is the cloud service provider for the government. They manage IT services for passport services, customs and other agencies. There is a new ICT act that is supposed to regulate ICT. But there is need for an overarching policy framework. We need wider participation and consultations in creating these response systems.

Comments (Professor Dunn): Public education is very important. We need to know that data are being protected. Public education is very important.

Final Session- ROUNDTABLE on NIDS

Prof Dunn opened the Roundtable with a may showing that many countries in the world are already using national ID systems, the issue for this Roundtable was not whether national ID systems are advisable, but how best to secure the data collected and how the process can improve security and national productivity.

Lead Presenter – Mr Carlton Samuels:

In Jamaica, the proposed National ID System (NIDS) involves capturing data from Jamaicans, about us, storing it securely, making sure access is managed effectively, and that data use can help transforms private and public interactions.

NIDS – 'One ID, Many Opportunities'. That's the primary document for verifying a person's identity. Benefits include authentication for digital services because it has electronic consistency. It is the basis for the digital economy and the information society. Public services can be delivered to eliminate fraud (as far as possible). The risk for ID fraud is lower. It meets the conditions for data protection. The problem that we have is that trust is ever changing. In order to trust we have to verify. There is the possibility of 3 factor authentication. In this regard, we need to move to biometrics.

Governance – National Identification and Registration Authority (NIRA) will sit in the OPM. There will be 19 board members. Security clearance for all board members and staff of NIRA will be vetted to ensure compliance. There will be a separation of interest; consent; transparency and inclusiveness; accountability; adoption of industry standards.

Security is at the architectural level. There are air-gap systems. Not all will be online compatible. The process level will have controls, for separation of actors. Every action is logged. There are also controls at the process level, development and operational levels. Blockchain technology will be used for log-ins. The gives transparency.

All persons using the system will be using 3-factors to access the system. Whether it's an iris scan etc. The system is designed for user audits. The security arrangement is pervasive and exist at all levels of the system. We are not supposing that the system cannot be breached but in the event of one it will be known to many persons.

One ID card provides 3 functions. We want to shift from High Risk to Low Risk IDs.

There are opportunities such as online on-boarding, signing contracts online, biometric authentication, financial inclusion and national end-to-end security.

For financial and banking systems that are virtual, citizens who are not online have been left out. NIDS would become accessible and bridge this gap.

Other benefits include enterprise data sharing (data subject consent required); certain conditions for data sharing; reduction of fraud and corruption.

STATIN has been looking at the national address scheme. It's difficult, for electoral lists. The better we are at managing addresses the better for managing the database. National Land Agency also will benefit.

Mr Julian Robinson MP:

Some of the criteria to be considered for implementing any national ID system includes:

1. Allowing for precise, accurate and unique identification;
2. Eliminating the possibility of identity duplication/falsification; or, at least, making both of those extremely difficult;
3. Making the means of identification easily accessible, both in terms of cost and number of steps required to acquire such means.

In the course of evaluating a national ID system, the specific context of each country has to be considered. The fact that a system works well in one country does not automatically mean such a system will work just as well if it is transplanted in another country. In evaluating a national ID system, one must first understand the ideological and constitutional context. Only on that basis can one properly go on to consider whether the objectives that can be considered common to such systems are met by a given system's particular configuration.

It is incontestable that large amounts of data will need to be collected and stored in order for a national ID system to meet the common objectives, i.e. precision, accuracy, reliability and integrity. But the starting point is a firm understanding (by those who will collect and store the

data) that the data does not belong to them and that they are therefore mere custodians of those data, it becomes apparent that the moral obligation on the collectors and custodians is to collect and store as little data as is needed to meet the objectives of the national ID system.

The data a national ID system collects will be in digital form. This has exponentially increased efficiency and convenience, but has correspondingly proliferated the attendant risks to data subjects. Many advanced nations have recognized this and appropriately responded with suitable legislative frameworks. A case in point is the GDPR, which came into effect across the European Union on 25 May of this year.

The bottom line is that no system is perfect, and the people who administer the system are as human and fallible as anyone else. Is there a suitably robust framework for deterring the very probable carelessness with people's data that carries very real prospect of putting them at untold risk?

Jamaica does not have any data protection legislation. The Bill for data protection has been stuck in a Joint Select Committee of Parliament for months. It is incumbent on those responsible to prioritise it, fix it and pass it. Only then will we have a suitable foundation for the design of a proportionate and constitutional national ID system.

Ms Judith Wedderburn (Civil Society):

The more I read about NIDS the more concerned I am about what will happen if it doesn't work. Human Rights Framework – In 2018 5 human rights declarations are being celebrated. The 70th Declaration of Human Rights is being celebrated on December 10.

National Identification and Registration (NIDS) Act (2017) was passed without a Data Protection Act. We need to have confidence in regards to the NIDS. I expect that breaches will be dealt with transparently. We need NIDS, but what do we do if there are breaches?

One of my concerns is the 'No ID', No Access' policy under NIDS. Without the NIDS will children access education? Public Hospitals will require a NIC. Why risk loss of life while

criteria are being determined? Will you be denied a passport without NIC? Is it ok if persons do not provide certain information under NIDS they will be criminalized? Is there no other way to achieve NIDS?

What is the role and opinion of the Minister to appoint members to the board of the authority? I welcome the fact that there are rules to preclude former MPs, Senators, or members of a municipality being on the NIDS board. What are the long-term benefits of NIDS? Press association of Jamaica (PAJ) is correct in its position, regarding threats such as disclosure of sources. There is an issue of the right to freedom of expression. The Jamaican constitution provides the right to protection of private and family life, and privacy of the home.

DNA, political affiliation and other sensitive information will not be collected. This is a positive benefit.

The ultimate test is ensuring that the system will lead to the trust and confidence by the general public. Citizens need accurate, adequate information to make informed choices about NIDS. There is much work to be done in this area.

QUESTIONS AND ANSWERS

Question (D. Donaldson - audience): NIDS would not be exempt from Data Protection when it comes on stream**.** What does it mean for citizens who wish to opt out of NIDS? If NIDS will be governed by Data Protection how does that work for citizens who wish to opt out?

Response (C. Samuels) Section 40 of the Act establishes the right for citizens to opt out. The regulation should allow for that issue. Section 42 allows for security.

Question (G. Mansingh - audience): The use of the data is important. How will the data be used? It could be beneficial to society. Most of the breaches arise in the banking system.

Response (C. Samuels) – Sections 42 and 43 allow for sharing of the data. But this has to be controlled and managed carefully.

Questions (audience): NIRA is a government entity and government entities are exempt from prosecution under the data protection act?

Response (J. Robinson) – The debate on the bill needs to be completed so that we can address that issue. At this point there is no Data Protection Act.

Response (C. Samuels) – According to the law the NIRA will be an agency in the OPM.

Response (J. Wedderburn) – Jamaica is a heterogeneous society. There seems to be the absence of choice. Your action by not giving the information is criminalized. We are contributing to a discussion of us and them. We need to have fulsome and honest discussion about how NIDS is going to affect trust in the society.

Question (audience): Why are we introducing a generation 1 system when we could introduce a generation 3 system?

Response (C. Samuels) – The systems in place are not generation 1. It's much more advanced than that. How you share data is a big issue. I agree that a system that is more beneficial and less criminalized would help. Choices were made, and based on the infrastructure and design, it does address security concerns.

Question (audience): Does the system allow you to release what you want to release or conceal what you want to conceal?

Response (C. Samuels): The biometric data could be pinned. But the card will have a data set, some of which is readable to you and others that will not be visible. But no, you will not be able to determine what companies can see when using the card. For authentication of your identity you have the ID card. NIDS itself is intended to be a

single point for authentication of identity. The idea behind NIDS is that you have a card that is authenticated.

Question (audience): If I sign up for the card, will I be able to retract the card? Will I have the right to be forgotten? The TRN has been introduced. Why are we discarding this system and what happens with this set of data?

Response (C. Samuels) - Under PICA you could decide you no longer wish to be registered as a citizen of Jamaica. There are processes built in for you to revoke and surrender the card. The regulations are not yet written and enforced.

Question (audience): Will I have the privilege based on the fact that I don't trust who I am giving it to, but will I be able to see each time there has been any access to my data?
Response (C. Samuels) – They will do a log in block chain technology to display the log, to see what has been accessed. That's one area of transparency that they are aiming to implement.

CLOSING PANEL COMMENTS

J. Wedderburn: Please follow up on the public discussions. Look at the constitution and your rights. Look closely at the NIDS legislations.

J. Robinson: We think the NIDS legislation as approved by Parliament is a bad law. It has been rushed. That's why it's before the courts. We believe the Data Protection Act should have been passed before passing NIDS. However, we are supportive of a national identification system.

C. Samuels: I believe we need a NIDS. The design and implementation plans mean that there is an opportunity to still address some of the concerns in terms of rights. It can be accommodated.

H. Dunn, Chair: Thanked presenters and in particular Mr Carlton Samuels for providing crucial information on NIDS. It appears that the panel agrees that the country needs NIDS, but that its legislation and implementation require continued public discussion.

In moving to close the Roundtable and the Conference, Prof Dunn thanked all presenters and persons for coming to the conference. He highlighted a recommendation that there should be an interim conference or consultation to talk about pressing issues rather than waiting for the next November conference.

Thanked the Partners and Sponsors for supporting the conference and all the members of the Organizing team from MICT CARIMAC, UWI MITS, RHQ and everyone involved. He said a report on the conference would be posted, as usual, on the website, as well as copies of all presentations and PPTs.

The 2018 Conference concluded with a sustained round of applause by the capacity audience.

MICT, UWI, November 2018