Rapporteur’s Report

7th National Cyber Security Conference

Mona ICT Policy Centre (MICT), CARIMAC, The University of the West Indies, Mona

June 18, 2019

INTRODUCTION

The 7th National Cyber Security Conference, hosted by the Mona ICT Policy Centre (MICT), CARIMAC, UWI, was convened at the UWI Regional Headquarters on June 18, 2019. This interim event was themed **Data Protection: What Next for NIDS?; Unpacking GDPR; Promoting Digital Productivity**. Following the 6th edition of the conference in 2018, one of the major outcomes was the need for the staging of an interim event to facilitate discussion around critical issues of cyber security. This provided the impetus for the 7th annual conference. The one-day event consisted of an Opening Ceremony and 3 plenary panel sessions featuring an array of expert local and international speakers. The Lead Organizer and Conference Chair was the Director of the MICT) Professor Hopeton Dunn, with partnerships from the Internet Society (ISOC), International Telecommunication Union (ITU), and the Canadian High Commission in Jamaica. Sponsors were National Commercial Bank NCB (Lead Sponsor), RJRGleaner Communications Group, the law firm Henlin Gibson Henlin, the Spanish Court Hotel and new sponsor Calibra Solutions Limited from Trinidad and Tobago. Over 120 registered participants attended the conference.

OPENING CEREMONY

Welcome and Opening Remarks by Professor Hopeton Dunn (Conference Chair):

Professor Hopeton Dunn welcomed all attendees, and in particular, the Principal of the UWI Mona Campus, Professor Dale Webber, and the Chief Technical Director of ICT in the Ministry of Science, Energy and Technology, Ms. Wahkeen Murray. She was representing Hon. Fayval Williams, Minister of Science, Energy and Technology, who was travelling overseas and sent her apology. Professor Dunn also extended special welcome to presenters visiting from overseas, including two representatives of ISOC: Mr. Shernon Osepa and Mr. Ryan Polk. Welcome was also extended to ITU's consultant, Mr. Gilberto Martins de Almeida from Brazil, and to Mr. Fredrik Ekfeldt, Deputy Head of Delegation of the European Union in Jamaica. All other presenters including those from the sponsors, were also specially acknowledged.

Professor Dunn highlighted that the interim conference was being convened in light of requests from participants and the decision made at the 6th edition of the conference in November 2018. He reiterated the conference's call for the Jamaican government to approve the Data Protection Act, which has been languishing since 2017 in the Jamaican Parliament. The consequences of not addressing data protection issues have wide-ranging implications for safeguarding citizen's rights as well as the private information on citizens and workers being held by government or corporations. Professor Dunn stated "What we are also talking about is ultimately the national security of our countries, and the future of establishing regional and international information systems". The theme of the conference was carefully selected based on national and international trends surrounding the increased impact of technology and the need for the protection of data at all levels.

Remarks by Professor Dale Webber:

The National Cyber Security Conference is an important landmark event within the Mona Campus. The work continues to shape and impact critical national and regional developments and with a deepened commitment to excellence. In 2019, we can no longer feel comfortable, leaving these matters to what was traditionally considered an elite group. And the fact that we are all gathered here, means that it is important to us all. 16 years ago, Facebook did not exist and politics was not done through Twitter. Crypto currencies were not in existence and digital assets have changed. Cyber security and data protection are important topics right now. While we grapple with organized crime, the networks that are there, our communities and or countries are at risk. Jamaica is in the 10% of countries around the world which have data protection legislation in draft. This draft was organized from 2017 but we want it to come out soon. Jamaica's National Identification System (NIDS) has aroused a lot of interest. General Data Protection Regulation (GDPR) is also of major interest. Especially those here at the University of the West Indies, where we have had discussions with our EU partners as well as with so many students whose identities as well as their data will now need to be even better protected.

I congratulate the Mona ICT team and all the stakeholders for planning and hosting such an important conference facilitating and sharing practices and fostering a community of knowledge, encouraging continuous training and retooling and most importantly providing a platform for collaboration.

Mr. Shernon Osepa, Manager, Regional Affairs for Latin America and the Caribbean, ISOC:

The ISOC believes in an open, globally-connected, trustworthy and secure internet. Presently, more than 90% of business in the global economy is being conducted over the internet. If we lose people's trust in using the internet then we have a big problem. In addition to this more than 90% of the global economy being conducted over the internet we can also see that just in 30 seconds more than two million US dollars are being generated over the internet. That is why we are focusing on promoting trust in the internet. ISOC has developed a trust agenda where we are focusing on cyber security, and related challenges that we are facing. The main objective is not solely on cyber security; the main goal should be: "How do we develop an internet economy in our country?" And by using technology, we can then achieve that. We must constantly ask: "How can we develop economic and social growth?" It is the ISOC's pleasure to contribute in making the internet a safe and trustworthy place for all.

Mrs. Nicola Whyms-Stone, Legal Counsel, Legal and Compliance Division, National Commercial Bank, Jamaica (NCB):

Conferences such as this, are very much needed because they not only help to educate but also provide a space for informed discussions that have the potential to inform public policies and to create a significant impact on industry practices. NCB is very proud to be a platinum sponsor of this very important event, as we are committed to using technology to streamline and digitize our systems. We are also keenly aware that increased cyber security and digitization go hand in hand. We believe that the protection of personal information and a secure processing of such data is very important to our customers. As such, we are more than prepared to be a part of events such as this that bring together local and international experts to discuss best practices and new ways to improve security data productivity.

The EU's General Data Protection Regulation, otherwise known as GDPR, came into effect on May 25th, 2018. It is perhaps the most significant change in data protection regulations globally in the last 20 years and has the potential to fundamentally change the way in which data is handled across every sector; from healthcare to banking and beyond. Although these regulations were approved in the European Union, their reach is global as they impact any company doing business in the EU or targeting the EU region with their services, regardless of where data is sent, processed or stored. The GDPR requires that personal information is protected. Because of the GDPR's extraterritorial scope, organizations in Jamaica must ensure that those who collect information are protecting it.

NCB has already taken several measures to safeguard its electronic data. One such measure is the RSA secure ID token. This helps to protect against internet fraud and scamming. This solution provides a unique code that along with your personal identification is required for your daily transaction. NCB has also provided their customers with the option to report any suspicious activities on their credit card through our portal. The website gives customers the power to block and unblock their accounts or to request a replacement card without having to go into a branch. NCB is working hard to be the bank of the future.

Ms. Wahkeen Murray, Chief Technical Director. ICT, Ministry of Science, Energy and Technology - on behalf of Minister, Hon. Fayval Williams, MP:

Data is important and every internet user has the right to the protection of identity from data theft, data breaches and protection of privacy. The Data Protection Bill is a significant piece of legislation that will usher in a new paradigm and provide a clear framework for the protection of people's personal and sensitive data. While there may appear to be some inactivity in relation to the Bill, I want to assure you that the Ministry has been working assiduously on it. Every single comment and recommendation made by the approximately 25-person joint select committee has been reviewed and the Ministry's recommendation have been submitted for consideration. It is the Ministry's intention to have the Bill passed in this current 2019 financial year.

So digital productivity tools have the potential to make technology work for us in the most efficient manner possible. However, of course the increased use of technology has its pitfalls. While we know that absolute security is illusive, we are committed to building a strong infrastructure and ensuring that citizens understand the risks associated with cyber space. In this regard the Organization of American States, through its International Committee against Terrorism has been working with the Jamaican Cyber Incidence Team to implement an early warning system with the installation of a security information and event management network. This network will among other things enable Jamaica to provide alerts as soon as there is a cyber-threat. An immediate response will be sent through the information technology systems in Jamaica. This system will certainly help us to be more proactive in our approach. The ministry will through its public education and awareness campaign, seek to reach 20,000 persons through targeted messages directed specifically for the group.

As technology continues to revolutionize every aspect of our lives, our responsibilities will be greater. In light of the Government's own efforts, the Ministry is extremely pleased with the discourse that has been taking place in recent times on data protection. In closing, the opportunity is taken to wish for the organizers of the conference and all participants a fruitful and impactful event. It is the Minister's hope that the discussions will facilitate the development of a robust data protection and cyber security framework in Jamaica.

Keynote Presentation – Mr. Gilberto Martins de Almeida, Legal Advocate and Consultant, International Telecommunication Union (ITU)

At least 58% of the countries in the world have data protection legislation. 10% of countries have data protection legislation in draft and 21% of the countries around the world have no data protection legislation. In Europe, the GDPR is a very strong piece of legislation. The GDPR is a major driving force on global standards. Many pieces of legislation around the world have been inspired by the GDPR. The Organisation for Economic Co-operation and Development (OECD) has published Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines have focused on risk management, which makes it much easier to implement. It has also focused on improved interoperability to address the global dimension of privacy. The EU Data Protection Reform Package is a modern legislative framework that supports international data flows with high protection. Many countries have submitted to the EU their pieces of legislation to ensure that their laws are sufficient, and many countries of different sizes have been highlighted for recognition. There is in place a Privacy Shied between the United States and the European Union, which allows different countries to apply for voluntary verification. In some jurisdictions it's difficult to pass a federal law and administrative bodies try to cope with this difficulty as is the case in the US with the Department of Commerce and the Federal Trade Commission.

There are global ISO standards that focus on privacy, and Article 43 of the GDPR provides for the adoption of some of these standards. So you can match the act with technical standards internationally. Personal data is the most targeted asset criminally, so we have a lot of important activity in this field. As a result of the GDPR legislation Google was fined US$57 million dollars for breaches of the legislation in France. Facebook was also fined 110 million Euros for misleading the European Commission on a Whatsapp deal in 2014. Most identity now is electronic. There is also a debate around Personal Identification Numbers (PIN numbers) and how secure they are, how regular should they change etc. Estonia is an impressive example: it's a country of less than 1.5 million people and has jumped impressively in the economic scenario, by the use of technological advancements. Nearly 98% of the population have ID cards, which is mandatory. That means they have different options of identification. 67% of the population use the card on a routine basis and it is estimated that 5 days per year is saved by individuals utilizing digital signatures. Proper data protection laws are key for this and for achieving social and economic goals.

SESSION ONE: Data Protection: Understanding the European Union's General Data Protection Regulations (GDPR)

Mr. Fredrik Ekfeldt, Deputy Head of Mission, Delegation of the European Union in Jamaica

The issues of privacy and data security are truly global; they are not confined to the borders of the European continent let alone a single country. The European Union's General Data Protection Regulation (GDPR) which entered into force on the 25th of May 2018 is the EU's response to the challenges and opportunities. Foreign companies doing business in Europe including the Caribbean companies are benefiting and will benefit from many of the on-going changes. It is not just a burden; it is an opportunity. These companies can now offer their goods and services in a harmonized and simplified regulatory environment in the EU, instead of having to deal with twenty-eight different data protection laws and twenty different regulators. Since May of 2018, one set of rules apply to their process operations and is interpreted in a uniformed way throughout the continent.

The GDPR is based on a modern approach to regulation which rewards new ideas, methods and technologies to address privacy and data security. The principle of data protection by design and by default recreate incentives to promote innovative solutions from the earliest stages of development. Investing in privacy pays off, increasing new commercial opportunities. Finally, co-regulator tools, such as code of conduct or certification mechanism are being introduced to help companies manage and demonstrate compliance.

What can the EU say after one year of application of this new rule? Has the GDPR delivered on their promises? Of course, one year is too short a time to draw a legitimate conclusion on the impact of the GDPR. We have seen some interesting trends that are very different from the scenarios that some are predicting and actually not materialized. To a large extent, the EU experience with the application of the GDPR has shown what data protection is really about;

simply sound data management, good business practices. This is mainly about having a culture of responsible use of data. Putting in place operational rules in assuring appropriate data security.

One of the main objectives of the GDPR was to give citizens more control and power over their personal data. The EU believes that it is important to raise citizen awareness in the field. This is why the EU has launched a campaign to encourage citizens to optimize their privacy settings. Today, more than 120 countries have data protection laws in place. Many of the new modernized laws tend to be based on common elements of comprehensive legislations, rather than on individual industries and services. This convergence is also taking place in Caribbean region.

Ms. Stephanie Williams, Attorney at Law, Henlin Gibson Henlin:

The focus of my presentation is on some key aspects of the GDPR which came into effect on May 25th, 2018, and to see how best we can gain some more knowledge about it. In Norway, complaints were filed against Google with their national data protection authorities on the basis that Google was processing their location data. At first glance, you may think: my location data? How can that be used to identify me? But when you look back, you can think about how your location information could reveal much information; it could identify you by your religious affiliation, your political affiliation as well as your health conditions. These are considered your personal data. Also, your sexual orientation, maybe if you are found in a certain location at a certain time, people might be able to identify your sexual orientation. Personal data must be relevant and not excessive in relation to the purpose or purposes which they are processed. The personal data should be accurate and where necessary be kept up to date. It should not be kept for any longer than is necessary. In our Data Protection Bill, there is a similar articulation of the standards for processing personal data. So we can expect that it may not differ much after it is passed.

The next issue that we spoke about is Privacy by design. This really means that it should become so innate in whatever system you are developing that privacy the element must be key and integrated throughout in order for it to have maximum benefits. One of the ways to protect a person's data is through encryption. Under GDPR, one of the things they have put in place is that there should be an encryption at the very least; in order to protect information of the data subject. The right of access one has to a data subject means you have the right to obtain confirmation that the entity you have given your data to is processing the data and you have the right to obtain access to it. Under the GDPR there are timelines within which persons are required to respond to a request or access to any data subject.

Under the GDPR, you are required to report any breach within 72 hours after becoming aware of it. You can be found liable if you breach. The standards to determine whether or not the GDPR applies to you, is whether you offer goods and services to data subjects in the EU, where you might be monitoring their behaviours. There are some of things that you need to do in your organization to ensure that you are GDPR compliant. The very first step is that you need a Data Protection Policy, and every organisation needs to have a handbook. Once you develop your policy, identify the persons responsible for its implementation and monitor compliance.

Mr. Ryan Polk, Senior Policy Advisor, ISOC

What's the state of online privacy concerns in 2019? In the 25 economies that we at ISOC surveyed, privacy concerns were very high across the board. Some 78% of the people surveyed said that they're at least somewhat concerned about their online privacy. Privacy concerns are growing year to year. Every year the majority of people have said that they're somewhat more concerned about their privacy than the year prior. So what are the sources of online privacy concerns that people talk about? The big one of course is cyber criminals. 81% of the respondents who are more concerned about privacy than they were the year before, pointed to cyber criminals as the source of this concern. Yet 74% pointed to internet companies as a source of concern: so you know your Google, Facebook. People are concerned about them when it comes on to online privacy. More troubling are the folks that point to their governments as source of concern: This totalled 66%, and that's not a small amount.

If you look at the ones that have the highest level of concerns in 2019 to the lowest level of concerns, privacy concerns were lower in the EU countries. Now there are a lot of reasons why this could be; it could be for instance just more knowledge or more understanding of what they are dealing with, with privacy or different ways they can protect themselves online but it also could be the GDPR that has an impact. In 2019 privacy concerns grew at a very low level in EU economies compared to the other economies surveyed. Some of them like Germany for instance only 26% said they were at least somewhat more concerned than the year before about their online privacy. That’s a really great result and something I’d like to see replicated globally. Has the GDPR had an impact on privacy perceptions in Europe? I’m not saying whether or not this is definitive because this is just a snapshot of survey results but these are interesting results nonetheless. In 2019 the EU respondents on average in the economies that we did the survey were 14% less likely to have some concern about their privacy versus respondents from non-EU countries.

Discussant: Ms. Arlyn Gordon- Representative, Jamaica Trade and Investment (JAMPRO):

Mr. Ekfeldt stated that it is important to manage your data flows within your organization. He has also spoken about how compliance with GDPR makes EU countries better prepared to deal with cyber security breaches. We have to think of what opportunities are presented to Jamaican companies and also the Caribbean as a region in promoting data protection. Mr. Ekfeldt spoke about the opportunity for Caribbean manufacturers who export goods and perform services in the EU, to benefit from being in a harmonized digital environment. A key for the GDPR is the personal power that it gives the citizen; citizens are now able to control how their data is being utilized by others and it also enhances the awareness of citizens to their privacy rights.

Ms. Stephanie Williams highlighted key aspects of GDPR and improving our knowledge of the data protection regulations. She spoke of protecting data through encryption and the pitfalls of storing data. She answered the question ‘How does GDPR affect Jamaican businesses?’ Mr. Ryan Polk of the Internet Society shared results of two surveys that were conducted in other jurisdictions. In Jamaica, do we really treat data protection as critically as we should? Do we really understand the need for our data to be protected? If we are going to draft a piece of legislation, we should do it properly and make sure everyone throughout the fourteen parishes of Jamaica feel and understand the effect of our data protection legislation.

Data protection is critical for us at JAMPRO. The EU has been described as the largest developed region market in the world. And it is an active market in which JAMPRO seeks export opportunities for Jamaica through the agency’s ongoing engagement with European investors. It is imperative for the agency that EU data subjects view Jamaica as a secure jurisdiction so far as data protection is concerned. We acknowledge the far-reaching effect of the GDPR and the penalties for breaches thereof. However, an interesting feature of the GDPR which ought not to be overlooked is that it serves to engender trust and confidence in doing business.

So, what are the implications for exporters to the EU? Businesses with less than 250 employees are exempt, unless they process personal data on a regular basis. SME's will simply no longer legally be able to add emails taken from business cards or link it to the email contact lists unless they have specific consent to do so, from the individual who gave them the card. Larger businesses must appoint a Data Officer. In Jamaica tourism entities need to ensure that consumers grant permission on any collection of data, for example on credit card information, birthdays, home addresses, marital status or next of kin on departure. This is encouraging a framework of transparency and it's engendering greater client and customer confidence, because it's going to keep the conversation going.

How can businesses prepare for the GDPR?

1. Train your staff to understand GDPR, ensure that they have consent to process personal data consent needs to begin for each specific reason for processing and it needs to be explicit.

2. You need to know what data is being held, where and how, as well as who is managing it. Check if appropriate consent has been obtained and whether the data should be processed or whether it should be deleted as consent had expired.

QUESTIONS AND ANSWERS

Question (C. Facey): How come China doesn't have a data trust issue? Is it because China is so highly policed?

Response (R. Polk): So actually we had the same question ourselves, so we also looked at data on trust. And internet trust in China was also extremely high. They were the highest there, and they also were not concerned about privacy. The one question was how we did the survey. We did the survey online. The internet as you know it, it is very policed in China, so I could imagine that at least Chinese respondents would be less likely to say things that would be critical of the government or critical of privacy, online.

Question: How would you define personal data?

Response (S. Williams): In defining personal data what they will do is that they speak not only to that individual the age, the name, or the picture. But if it is that you have any information that, when put together as composite is able to identify you; then it would fall under the regulation. And a similar scheme is being proposed in our Data Protection Bill. In circumstances where you have big entities who collect various bits of information; when you put it together as a whole, it can also be considered as personal data.

Question: I'm not quite sure if we got the distinction between data and sensitive data, and sensitive personal data. I would like you to make that distinction and basically clarify for me.

Response (S. Williams): One of the distinctions in the proposed Bill and also in the GDPR, is that there is a different level of protection that is required for each. So, for the sensitive personal data there's a higher threshold and there are more steps and procedures that you have to put in place to protect it. For personal data, generally speaking, we're speaking about your name, your age, your sex. When they get to sensitive personal data, the example that they give is genetic biometric health data and those on religious and ideological convictions. Those are the examples or the category that's sensitive personal data. So that is really the distinction. The personal data is general information, but the sensitive part comes in when we are speaking about genetic information, religious affiliation, political affiliations and biometrics.

Question (D. Donaldson): I'm quite concerned about the distinction, if there is any attention today in terms of Government data which has protected computers, how broad will that scope be? How would you define that? And in terms of the timeline for breaches to be reported, from a law enforcement perspective.

Response (S. Williams): In the proposed Data Protection Bill, from my recollection there is a specific timeline within which you are to report. The timeline is 72 hours in the GDPR but I don't recall the proposed timeline within which you are to report. Certainly, that is something that we might have to put forward to say that should be amended. In terms of the government I do recall that there is a provision that speaks to government entities being exempt to a certain extent. I believe that was one of the issues raised by persons to say, there are a number of government entities subject to collect information; why are they not subject to the same regulations?

Comment (T. Forrest): NIDS is a different thing from the Data Protection Bill. What does the Data Protection Bill prescribe? You have what's called the Office of the Data Protection Commissioner or Information Commissioner's Office. They are still deciding what that's going to be; as in the name. But that office is where you go to if you have any concerns or complaints. As it relates to exemptions, there are exemptions but they are prescribed and they are not total.

SESSION TWO: Promoting Digital Productivity and Online Security

Session Chair, Mr. Clyde McKenzie, Specialist, Cultural and Creative Industries

Those of us familiar with some of the challenges faced in the digital sphere will understand that productivity and security operate in tandem, because sometimes you have to space one in order to accommodate the other. We all know that in the real world many of these developments are mediated by political considerations. Sometimes technological outcomes do not necessarily follow the intentions. And so this afternoon, we will be looking at how we balance issues of digital productivity and some of the risks that we might face in trying to achieve this objective. We have assembled quite a distinguished panel to address this particular topic.

Professor Hopeton Dunn, Technology Policy Analyst and Director, Mona ICT Policy Centre (MICT), CARIMAC, UWI

There are now 4.3 billion users of the internet representing 58.8% of the global population in 2019. This means that almost half of the world is still not connected. There are parts of the globe that do not have access to the internet, an issue that is known as the digital divide. In our own Caribbean region, when we talk about connectivity and we think about Haiti, we are talking about 12% internet penetration, compared with an approximate 40% for the wider Caribbean region, with country variations. There is some way to go and if you look at some of the details of that you will see that there are some countries that are doing much better than other countries. Jamaica based on some studies which we have been done over the last year or so in about 67% internet penetration. All of this is taking place in the context of what has already been referred to from this platform as the Fourth Industrial Revolution (4IR). Most of you will know that it is also referred to as 4IR, a system that is blurring the lines among the physical, digital and biological spheres. 4IR is heavily reliant on digital applications in the delivery of services including algorithms and robotics. All of these things cannot operate without a strong people base, a trained workforce with an understanding of the values needed to enhance digital productivity.

In terms of productivity and business benefits, businesses are taking advantage of Artificial Intelligence (AI) technology by reducing operational costs, boosting efficiency, increasing resources and improving the customer’s experience. AI empowers companies to save time and money by automating redundant processes. However, regrettably, it is also being used online to undermine people’s identity and to create a false images. Technology is a two-edged sword. One of the ways in which we see this fictional element that can be a detraction from productivity is what is known as “deep fake”. Many of you “techies” have already encountered and are quite familiar with the notion of deep fake. I know that we have diversity in the audience, so when I speak about AI-based technology, this is technology used to produce authentic looking video or audio content by digital manipulation to create false images, speech or scenes. This is not just Photoshop: it is way beyond that. So you see that things might not be what they appear to be and you can imagine the impact and implication of this for people who are involved in digital media productivity for authentic news and information presentations and election coverage and providing educational content. (Short video screening on examples of deep fake)

On the more positive side, adaptability, creativity and security will enhance genuine digital productivity on any internet platform or tool. But we have to be aware of some critical policy changes that can affect digital productivity: One is Net Neutrality where we are demanding uniformity in internet speed for all online users and no two track system based on location or ability to pay. Another is Digital Switchover where we have to ensure that our productivity and media systems are compliant with ITU requirements for transitions from analogue to digital. Yet other area that we need to think about is the growth of gig economy and how it is disrupting some traditional service providers, whether in generic website design, Uber taxis or Airbnb accommodations apps. Agile new companies are now disrupting some of the traditional companies in offering the whole range of services in a non-traditional way.

However, we must plan strategically for transformation in digital productivity not just for disruption. We need to look at new training subject matters. For example we should be teaching such courses as entrepreneurship for digital innovators, data analytics, AI applications for business and science, ethics in science and technology, data protection and cyber security, emotional intelligence, critical thinking, and effective digital communication. These are some of the things which across the board our institutions need to be taking into consideration.

New approaches are required, such as recognizing that power is changing hands from dying hierarchies to living networks. To enhance digital productivity, start-up and innovative individuals must understand that productivity does not proceed by age or status, but by digital competences. We have to engage in what I have been calling Globalization from Within. That is starting with available internal resources but with self-confidence and a strategic plan to go global, using the internet, 4IR and other digital 21st century productivity tools.

Mr. Douglas Halsall, CEO, Advanced Integration Systems Limited

I must start by commending the professor for his insightful presentation. Those are some of the things we need to be doing to make it on the global stage with technology. I have fortunately been associated with a number of firsts in Jamaica: the first ATM, the first CXC for Computer Science, the first time the university changed from punch cards to UNIX, the supercomputer at Mona Informatics and the following industries that went into technology – credit unions, general insurance, government accounting, Air Jamaica, hotels in Latin America starting with the Pegasus. Today I talk to you as an entrepreneur.

We are living in the exciting age of mega digital platforms. My company operates in many different countries. Because we process many financial transactions we have to be PCI (payment card industry) compliant. We also process numerous the insurance claims in Jamaica and the Bahamas, so we are fairly acquainted with the matter of security. Locally, our Provider Access System (PAS) is connected online real-time to 5000 healthcare providers: all the doctors, all the pharmacies in Jamaica, all the labs, all the hospitals. We process 1.3 million cards, excluding the ones in the Bahamas. We process 130,000 claims online real-time every day, and we have a copyright on certain drug codes for the Caribbean. 20 years ago we decided that our drugs were coming from all over the world and there was no standardized coding structure. So we worked with a partner out of Germany and today we have over 8000 drugs coded for the Caribbean from all over the world.

The National Health Fund for example can manage their drug programme, including the quantity of drugs given for any particular disease. This same system that we have at the National Health Fund, in 2010 won the computer world laureate prize as the best such system in the world. So think not of just being a follower, think, why not compete with the world. Today we have succeeded in digitizing the first hospital in the Caribbean, and that is the University Hospital of the West Indies. Our goal is to have real-time information health systems, which will allow patients to access their medical records where ever they go. We're moving toward tele-radiology, electronic prescriptions and remote care.

A major problem with tele-medicine is that less than 14% of Caribbean people have credit cards. Over the past 5 years, my company, Advanced Integrated Systems, (AIS) which spends 20% of its profits on research and development, has spent over 5million US dollars on a mobile money platform and some allied systems that will drive transactions. Using the brilliance of your next speaker as our lead programmer, we'll be releasing in the next two weeks, an Amazon lookalike for local merchants. That will address the absence of credit cards. We are implementing these innovations over decades and reaping the benefits for industry and public sector in Jamaica and the Caribbean.

Mr. Christopher Gayle, CEO, Gizzada Software Limited:

I started programming the year the first IPhone came out – 2007. When I started, mobile devices weren't as powerful and the data was far more limited. In 2007 I started this website called Buildyourownnetdream.com and this website was pretty much filled with fun fan-made games and we all played for a bit and wanted to figure out ways to add features of our own. In this simulated world everyone is connected, communicating, trading, collaborating, feeling and this is all digital. As the years progressed and I was working on this it became obvious that the things we were making could be applied to the real environment around us especially because mobile devices and data were making what we can do in this simulated world accessible, because everyone is connected.

I wanted to develop things that would cross all the different platforms and as I learned more and more I became a little concerned because we need best practices in order to survive today. We are now a lot more connected and at the same time exposed to a lot more risk. Here are a few tips on cyber security: we have to adopt habits that are going to keep us safe; We need to take care of ourselves digitally. We are all targets. You need to have good password protection habits. Don't leave your devices unattended; Always look at links carefully before opening. Do not use free Wi-Fi all the time for personal matters. Back-up your data regularly. Don't plug things into your computer as much as is possible and don't use your thumb drive in strange places. Be wary of unnecessary risk. Monitor your online activity.

We can start to use the technology to become more productive and to feel fulfilled. Automate things that are monotonous to ensure you are productive. It didn't take much genius to build what I've built thus far, it just took a lot of hard work. Knowledge and expertise are now being shared across the globe at the speed of light because of the internet. Because one has these devices in their pockets. We need to focus on making these things available to everybody.

QUESTION AND ANSWER

Question (unidentified audience member): How do you protect your websites from certain risks?

Response (C. Gayle): I try to minimize how much data I expose whenever people visit my site so that very little information is accessible for them to try and do anything to us. But you still have to look out for attacks and stuff like that but I think that anyone in the sector will face similar risks. We have to be ready to react.

Question (T. Forrest): How do you see the role of academia in helping to change our mind-set and get us ready to exploit opportunities?

Response (Professor Dunn): I am glad you raised that question. Last year I gave a presentation in the Dominican Republic where I critiqued the academy in terms of its fitness of purpose in the 21st century. Academia will have to make certain decided shifts in how it operates to create professionals and persons who can operate in a flexible 4IR environment going forward. For example, academic institutions are divided up into silos called Faculties but the way to learn is in this era is to learn across multiple disciplines and faculties. So we will have to engender some fundamental institutional changes and those changes will also have to acknowledge the fact that learning takes place in multiple directions. You can enter a class as a professor but know that you are not the ultimate authority on the entire subject anymore. There are young people in there who may know more about aspects it than you, and your job is to empower them to become the best they can be and surely better than you.

SESSION THREE: Data Protection: What Next for NIDS?: Understanding the Supreme Court Ruling and Looking Ahead (Round Table Session)

Session Chair Mr. Damian Donaldson welcomed all audience participants to the session and introduced members of the roundtable panel to speak in the order as on the Conference programme.

Mrs. Georgia Gibson Henlin QC, Attorney at law, Henlin Gibson Henlin

What constitutional rights are being violated by NIDS? It is important to appreciate whether the challenge was about ‘Is the system good for Jamaica?’ Or whether it was something else. My question on reading the judgement is not whether we want a national identification system. In fact, in starting out at paragraph seven of the judgement the judges pointed out that there was common ground between the claimant Mr. Julian Robinson and the respondent - the Attorney General, that there are benefits to a NIDS. But the challenge was more about how it was going to be implemented and how it would impact our constitutional rights. So what are the rights that were being violated? The equality right under the constitution was impacted. Whereas it was compulsory for citizens and residents to obtain national identification cards in order to access services, foreigners could come and not be registered at all and access those same services.

The other right that was violated was the right to life, liberty, security of the person under section 13(3A) of the Jamaican constitution. This is primarily because of the compulsory nature of the registration and there was a risk of prosecution if you refuse to be registered. They also said that the fact of prosecution does not take away the risk of further prosecution because it is a continuing offence. The other right is the right to privacy that is protected by the constitution. That one resonates with me because you can see the link between that right and the data protection legislation. Chief Justice Brian Sykes was careful to ensure that readers understood the Supreme Court ruling. He went out of his way to try to explain what biometric information is and how it is used and the technical underpinnings of it. He also went to India and brought that jurisprudence to bear on our law. All the court is saying is that we are a constitutional democracy, we have rights, privacy is an important right and we have to get it right and the government has a greater obligation than anyone else. Unlike in India where a lot of data and research were brought before the court to show how it would work, that wasn't done here. That is in part why the challenge succeeded.

Mr. Julian Robinson, Opposition Spokesman on Science and Technology

The reason the PNP pursued the court case and the reason I decided to be the claimant in the case is that I decided that the law that was passed fundamentally breached our constitutional rights. And I made a point to separate the issue of a National ID from the law. We are in support of a national ID and I'll outline how I believe we can go forward with a national ID. But we strongly felt that the approach taken by the government in developing the NIDS Act was wrong in terms of the lack of consultation on the law specifically. There were a lot of consultations about the systems and the benefits of the system but we were adamant that it should go to a joint select committee of Parliament which would allow all Jamaicans to participate and it didn't. What was passed, as the courts have upheld, breached our constitutional rights. How do we go forward?

The new Minister of Science Energy and Technology has given a commitment to set up a joint select committee to discuss the Data Protection legislation this month (June 2019). It is important that we conclude that before we implement NIDS. Because it safeguards the rights of the owners of data; how that data is going to be accessed; who that data can be shared with; and how it can be used. So that's the first thing; we must have Data Protection legislation passed before we move to NIDS. Secondly, there has to be some data sharing policy or framework across government. Currently government has a lot of data on us; for example the Registrar General's Department (RGD) where all births and deaths are recorded. If you take the Electoral Office of Jamaica, they have your finger print and they have your facial data so there is already data there. Should the

Police Force have access to the finger prints that the Electoral Office of Jamaica has? The EOJ has over two million people registered in its database. Of course it could help in crime fighting. Is that an option? The current law doesn't allow it, but that's an option we should look at.

It's important that whatever data we are asking of individuals, that the data is necessary for the reason it is being collected. We felt, and the court upheld, that the level of data that was being requested from NIDS was just too intrusive; fingerprint, toe print, iris scan, etc. The question is whether you need to have that level of data for a national ID. Going forward, a national ID shouldn't be compulsory and then you have criminal sanctions for persons who don't participate. What you have to do is build incentives to encourage people to participate. And you can find ways to incentivize it as they do in Estonia, such as discounts for public services. The Electoral Office of Jamaica already collects data for over 2 million individuals over the age of 18 years. By the end of this year they will be issuing a card that will have biometric information on it. We should build on that. In essence it acts as the ID. We don't need to reinvent the wheel. So how do you treat with people who are under 18? Everybody who is born has to be registered at the Registrar General Department (RGD) office. There is data you have to collect there. You can build on that capacity to develop an ID for persons under 18.

So the system has to take account of data that already exist, make the data collection voluntary with incentives to participate, and we should proceed first with the Data Protection legislation before any re-enactment of a national ID system.

Senator Robert Morgan, Parliamentary Secretary, Office of the Prime Minister:

The first time that we ever thought about a national identification system in Jamaica was in 1982 when there was an exploratory committee set up under the leadership of J.A.G. Smith. He gave a report in 1982 and a lot of the recommendations that were in the bill in 2000 and the bill in 2017 came out of that period 1970-2011, when the NIDS project was at the Ministry of Health. In 1993 Cabinet approved the establishment of the National Registration Unit. In 2001, the bill was referred to a Joint Select Committee but fell off the order paper. It wasn't passed because there was a contention on whether you could force father's names to be included on birth certificates. In 2017 the bill for NIDS was tabled and passed but in 2018 there was a constitutional challenge by Mr. Julian Robinson and the NIDS was declared unconstitutional, null and void.

The government of Jamaica is committed to the implementation of a national identification system. A decision was taken not to appeal the judgement of the constitutional court. Why do we need NIDS? It will provide Jamaicans with one ID which is reliable, secure and verifiable. Currently we have a myriad of identification documents: Passport, TRN, Farmer's ID, NIS, Voter's ID, PATH ID, School ID, and Driver's License. The purpose of a secure national ID is to increase the ease of doing business, to reduce identity theft, to bring Jamaica into the digital economy. Some 80% of the funding for NIDS is actually to upgrade the government's ICT framework, which will create a unified system across government.

The government will retain its broad policy and will continue implementing non-NIDS activities, while developing new processes to deliver fully-digital services. The government is also committed to continue its consultations with stakeholders regarding the NIDS legal framework and benefits. Public education is another key goal that the government will continue.

Ms. Nicole Foga, Managing Partner, Attorney at Law, Foga Daley and Company:

A digital identity is now being seen internationally as a prerequisite for individuals and businesses to access government services, participate in a knowledge-based society and digital economy. A digital identity allows government to improve service delivery, offer new innovative services and engage with their citizens in a streamlined and efficient manner. That we have to accept. Where the court case takes us legally is that firstly, the legislation failed on the basis of the absence of data protection provisions. There was an over-reliance on regulations that would address glaring deficiencies, and of course the numerous breaches to the constitutional right to privacy. Socially, there was an absence of stakeholder buy-in. I was not aware of any group of citizens clamouring for the implementation of the system. The system was seen as a burden not a benefit, and there were a number of concerns being raised.

The way forward has to be more about stakeholder buy-in, more engagement, because there are benefits to a digital system and we can't pretend that there aren't. We have to be concerned about hacking and rising costs, but not enough discussion had taken place on the benefits for citizens to gain from this system.

Mr. Carlton Samuel, IT Consultant and Specialist, NIDS

It is good public policy to have identity systems that allow one person to be identified as that same person. We all agree on that. Identity is dynamic and variable. You also heard about the challenges we face in participating in the digital economy and society. When you think about identity which is dynamic and you think about digital identity which is one of them, then you see where the challenge is. Digitization expands everything we think we know about digital identity. Sustainable development goal 16.9 of which the government of Jamaica is signatory, commits the GOJ to have a legal identity for everyone in Jamaica by 2030, and that legal identity is digital. So we have to traverse all these identification systems at low risk. The digital identity has the lowest risk available to us. We therefore have to define individuals as who they are. The only way to do that is to include some biometric information. We can't escape that. That is the single way we can unerringly say you are who you say you are. The technology to identify a single ID for a single person is on hand. The NIDS platform is configured with the technology that allows us to do that. We have a way to secure it. But it must be online to make it valuable. We have to ensure that the civil registration is fit for purpose.

If you go to the Registrar General's Department, particularly in rural areas, can anyone guess what is the least reliable picture ID presented for name? The Voter ID. The civil registration process enables national identification and the national ID enables the civil registration process. The challenge is not technology. We have the technology today. The dynamic of the identity business is about governance, operations, law, practice etc. We have to decide what we mean when we say we want to include people socially. Identification systems in the digital world speak to each other and a single identity must be able to navigate all of them. Identity is dynamic. Just about everywhere you travel will require e-passports and we have signed on to international regulations that compel us to have e-passports. If you don't have an e-passport you won't be able to go across a national border. The question is are we going to facilitate us moving across national borders before we facilitate us moving between systems? That is the question.

QUESTIONS AND ANSWERS:

Question (D. Donaldson): In terms of providing assurance, how do you envision convincing the people and ensuring that everything is in place to adequately protect their data?

Response (C. Samuels): If you look at what was envisaged for the NIDS, There is the PKI (public key infrastructure) and the private key. They have to work as binaries. There is also encryption. It is not fool proof, but the technical infrastructure is implementable and available.

Response (J. Lynch-Stewart): A part of the whole system is you protecting yourself, because when someone wants to verify who you are, you have to give permission. Someone cannot verify who you are without your permission. You also have control of your data.

Response (N. Foga): Based on what Chief Justice Sykes was saying, you will still have to address what is contained in the database and whether it is voluntary. His position is that no system is fool proof and what would be the implications if there was a hack.

Question (I. Reid): What would persons in a rural area have to give up to get access to NIDS card? In order to provide access to information, would persons have to sign a disclaimer for an institution to access information? If it will cut down on crime, how will you get the violence producers to sign up for a NIDS card?

Response (G. Gibson-Henlin): The Data Protection legislation will allow citizens to control how their data is used. As it pertains to the violence producers, when something happens in the US it is so much easier to identify the criminal. In China they have some technology that narrows it down to the face. I don’t agree with it being as invasive as that, but I think that’s where they are trying to get where the more information you have on people the easier it is to fight crime.

Question (Unidentified Audience Member): Is there a digital platform that encourages end-users comments or feedback on NIDS?

Response (NIDS Team Member): So we have NIDSFACTS.COM and we have a portal in which you can submit your feedback

Question (Unidentified Audience Member): After receiving these questions and comments what happens? Is there a review of the suggestions or the comments?

Response (R. Morgan): Over the last three years we have gotten hundreds of comments and we had to hire someone to go through the comments and respond to everyone.

Response (J. Lynch-Stewart): Under the previous law there was supposed to be an 18-month period for review. So what we had developed is an 18-month file within our office with all of the suggestions from people and we would have put all that together to go back to the policymakers to say this is the feedback we've been getting from the population. Now that the law is null and void, we are still going out to get feedback. Once the new bill is tabled in Parliament we will publicize it to get their feedback.

Question (Audience): How do we ensure that customers data is protected, is a Privacy Impact Assessment done? Is there a process for citizens requesting the data on other citizens?

Response (C. Samuels): The standard procedure is to have a Privacy Impact Assessment done on any digital system that is implemented. So NIDS will definitely have it implemented. In this dispensation for NIDS, one of the things that we had proposed is that we use block chain technology to literally tell you when anybody has accessed your data that is held on the platform. So you will get a notification of access. That is one step above a breach notification. Systems will also be audited to ensure they function properly.

Comment (T. Forrest): The problem people have with NIDS is not giving information, but what happens after the information is given. Nobody trusts anybody in these state-run facilities to treat with their data in a safe and sound manner. The technology can help build that trust. Establish trust between citizens and the gatekeeper. Block chain will help with that. So you can trust the system. Data self-sovereignty is important where you must have control over your data.

CLOSING REMARKS:

Professor Dunn thanked the Session Chair Mr. Damian Donaldson for his coordination of the roundtable panel discussion and all session chairs throughout the day's conference proceedings. The audience was also warmly thanked for their attendance, including new attendees this year and those who have been attending over several years. All 17 presenters were thanked for participating in the conference and special appreciation was expressed to the 4 international presenters who participated. Professor Dunn noted that it was good that the University of the West Indies is playing its role in this way, and he expects that it will continue to do so.

The organizing committee for the conference was thanked for their support: Ms. Danielle Insang, Conference Admin Assistant; Mr. Al McLaren, Technical Services; Mrs. Paulina Plunkett Gray, Sponsorship and Finance Admin; and Mr. Alpha Obika, Programming Support and Rapporteur. MITS and the UWI Regional Headquarters were thanked for providing live coverage on UWI Mona Media and hospitality services respectively. Special thanks was extended to the National Commercial Bank for their lead sponsorship, as well as to other sponsors: Henlin Gibson Henlin, RJR Communications Group, Calibra Solutions and Spanish Court Hotel. In closing Professor Dunn thanked everyone for continuing to make this conference series happen so smoothly and with such large and diverse attendance. He said this kind of dialogue was crucial to the national conversation on technology, public policy, research insights and digital security.

The comments were affirmed and the event brought to a close with rousing applause.

Report Produced by Conference Rapporteur Alpha Obika with assistance from Roxanne Morris.

MICT, UWI, June 2019.