

# Trinidad and Tobago Internet Governance Forum (TTIGF) 2019

*The Internet of Trust*

## TTIGF

TRINIDAD AND TOBAGO

INTERNET GOVERNANCE FORUM | 2019

# The Internet of Trust

JANUARY | 25<sup>TH</sup> | 2019

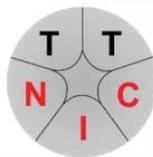
AT

TT CHAMBER OF INDUSTRY AND COMMERCE

9:00AM



Internet  
Governance  
Forum  
Support  
Association



PARTNERS



lacnic



January 25th, 2019

Trinidad and Tobago Chamber of Industry and Commerce  
Port of Spain, Trinidad and Tobago

## Overview

The third annual **Trinidad and Tobago Internet Governance Forum (TTIGF)** took place on January 25th, 2019, from 9 AM to 5 PM at the Trinidad and Tobago Chamber of Industry and Commerce, Westmoorings, Trinidad and Tobago. The theme of the TTIGF for 2019 was “The Internet of Trust.”



There were 85 face-to-face attendees including panellists, special invitees and TT MAG Directors, and 270 views of the livestream via YouTube.

The structure of this report follows the format of the TTIGF 2019 event, with four sections:

- Introduction and Opening Remarks
- Panel Discussions
- Open Forum
- Conclusion

## Hosts

TTIGF 2019 was hosted by the Trinidad and Tobago Multistakeholder Advisory Group (TTMAG). TTMAG's mission is to be an independent entity for the promotion and development of best practice policy standards for the .tt country code Top Level Domain (ccTLD) and the local Internet ecosystem in the interest of the Internet Community.

The TTIGF would not have been possible without the support of its strategic partners: AVIT Ltd., Internet Governance Forum Support Association (IGFSA), Latin America and Caribbean Network Information Centre (LACNIC), L'Onction Friandises, the Trinidad and Tobago Network Information Centre (TTNIC), Trinidad and Tobago Internet Exchange Limited (TTIX), and WiPay (Trinidad and Tobago) Limited.

## Resources

### TTIGF

Website: <http://igf.tt>

Email: [info@igf.tt](mailto:info@igf.tt)

[Twitter](#), [Flickr](#), [YouTube](#)

### TTMAG

Website: <http://mag.tt>

Email: [info@mag.tt](mailto:info@mag.tt)

[Twitter](#), [Facebook](#), [Instagram](#), [Flickr](#), [YouTube](#)

## Introduction and Welcome Remarks

To open proceedings, [TTMAG chair Dev Anand Teelucksingh warmly welcomed both in-person and online participants and delivered a brief address](#), introducing the three themes of TTIGF 2019, namely Caribbean Data Protection Regulations, Cultural Factors in the Caribbean Affecting Trust & Privacy for Digital Security, and Using Technology to Increase Trust in Public Institutions. He also informed the audience that outputs from the previous two iterations of the TTIGF were shared at other regional IGFs including the Caribbean IGF (CIGF) and the Latin American and Caribbean IGF (LACIGF), as well as the global IGF. Further, the TTMAG hosted an internet governance educational session, Internet Governance 101 in July 2018, and hosted a remote hub for the global IGF 2018 in collaboration with the Telecommunications Authority of Trinidad and Tobago (TATT) in November 2018.

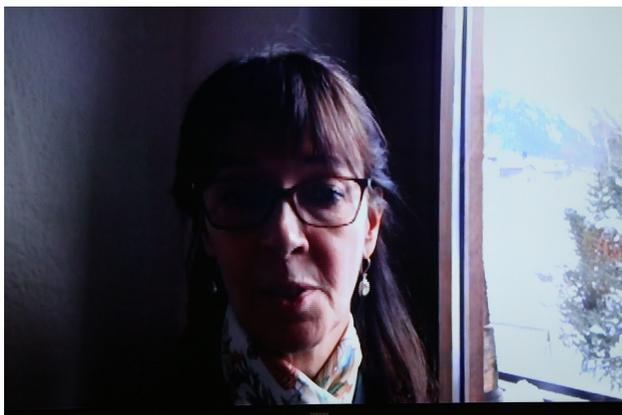




Chair of Proceedings and TTIGF 2019 Convenor, Tracy Hackshaw gave a brief introduction and history of the IGF process, then introduced recorded welcome remarks from the following global internet governance leaders:



- [Ms. Lynn St. Amour, Chair of the Multistakeholder Advisory Group of the Internet Governance Forum \(MAG\);](#) and
- [Mr. Jovan Kurbalija, Executive Director of the High-Level Panel on Digital Cooperation.](#)



Mr Hackshaw then introduced the first panel discussion of the event, on Caribbean Data Protection Regulations.

# Panel Session 1: Caribbean Data Protection Regulations



Caribbean Data Protection Regulations (CDPR) panel (L to R): Mr. George Gobin (moderator), Dr Yufei Wu, Mr Bartlett Morgan, Mr Darren Mohammed, and Ms Vashti Maharaj.

## Moderator

Mr. George Gobin, Director - Trinidad and Tobago Multistakeholder Advisory Group

## Participants

Ms. Vashti Maharaj, Head, Legal Services - Ministry of the Attorney General and Legal Affairs

Mr. Darren Mohammed, Corporate Business Manager, Caribbean/Country Representative - Microsoft Trinidad & Tobago

Dr. Yufei Wu, Associate Professor and Coordinator - Caribbean Institute of Cybersecurity

Mr. Bartlett Morgan, Associate Attorney at Law - Lex Caribbean

## Introduction

Mr. Gobin introduced the panellists then introduced the topic with reference to the European Union's General Data Protection Regulation (GDPR) as well as recent cases brought against internet giants

Google and Facebook relating to the protection (or lack thereof) of user data. He seeded the conversation by asking “who is responsible when someone in the Caribbean gets hacked? What happens to their data?”

## Introductory Remarks

Ms. Maharaj explained that the idea of data protection regulation generally, and “CDPR” specifically, is very broad. While the panel topic refers to CDPR, there is at present no CDPR regime or regulation, though it is something very much touted and needed, as the EU through GDPR represents a united front where governments have a harmonised approach. She indicated that this is something that CARICOM should look into.

What do we have in our regional space that advocates for regional data protection? At present, Ms. Maharaj explained, the following is what exists:

- CARICOM Single ITU Space: one aspect is harmonised legislation with regard to ICT - a mechanism for dealing with E-Transactions, E-Commerce, Data Protection and Privacy
- CARICAD and other regional ICT bodies

She then noted the statistics on data protection regulation in the Caribbean. **68% of the countries in the Caribbean do not have data protection legislation.** Of those that do, including T&T, the Bahamas, Jamaica, Barbados, St. Kitts and Nevis, St. Vincent and the Grenadines, and Antigua and Barbuda, many of them are outdated. Moreover, new technologies put legislation to the test. In addition, data protection is not an isolated phenomenon or policy domain, and Ms. Maharaj asked, “what is the impact of technologies such as AI, Big Data, Cloud, IOT on a potential CDPR regime?”

Mr. Mohammed opened his contribution by detailing Microsoft’s role as an information controller as well as a data processor under the rubric of the GDPR. This entails 4 contexts relating to trust, namely:

- **Security:** encryption of data
- **Compliance:** with regulations, including GDPR, ISO 27001, 27018, FSMA, HIIPA as well as sovereign regulations

- **Transparency:** telling customers where data is hosted, where the backup is located and how data is treated with
- **Privacy and Control:** Customers' data is their data, not Microsoft's - treating with law enforcement requests by putting them back to the customer; Microsoft will always turn data requests from law enforcement back to the customer.

Mr. Morgan expressed his gratitude for the convening of a panel on such an important topic. It allows the Caribbean to take stock of and plan towards engendering trust. He detailed that perhaps the HIPCAR efforts towards model legislation can be modified but its essence maintained and suggested that this idea could be discussed in the panel. He noted also that the EU-CARIFORUM Economic Partnership Agreement (EPA) also gave a time frame for the implementation of data protection legislation as a condition of the agreement, though many people aren't aware of this.

Dr. Wu presented on the Cybersecurity Aspects of GDPR, and provided a useful summary of key clauses of GDPR, including

- Clause 5: How are you protecting against unlawful access to personal data?
- Clause 24: How are you ensuring and demonstrating data protections?
- Clause 34.2: What steps have you taken to protect against external threats of unlawful access, disclosures or loss?
- Clause 32.4: What steps have you taken to protect against insider (ie. employee) abuse of personal data?
- Clause 35: Can you detail and disclose a data breach within 72 hours of the breach?

He outlined the responsibility that lies with individual organisations to monitor and implement these provisions under any data protection and noted that organisations, once they have users in Europe, could be subject to GDPR. Fines of up to 2% of global turnover could be levied for breaches of GDPR. He also posed the question of how Caribbean countries would treat with these 5 responsibilities?

## Updating Legislation

**Question from Moderator: How to help solve the issue of 68% of countries not having data protection legislation? Do we really need it?**

Mr. Morgan offered a legislative perspective though he indicated that the full conversation is all-encompassing and not only legislative. He outlined 3 major options or approaches to treating with data protection legislation:

- A treaty-type approach to data protection, where each country implements aspects of it that are relevant to their needs and situations (e.g. the Treaty of Chaguaramas);
- HIPCAR model; model legislation that can (in theory) encourage Caribbean countries to implement provisions; or
- Leaving it up to each individual state to do what it pleases; it is the default if nothing deliberate is done.

He continued, saying that the reality of small island developing states (SIDS) is that government has to and does remain at the commanding heights of major issues, especially legislatively, though the hope is that the approach taken is more inclusive than government-only.

Mr. Gobin noted that when the Treaty of Chaguaramas was drafted, online services didn't exist and many forms of information sharing didn't exist, so we in the Caribbean have to move with the times and update provisions to suit new realities.

Ms. Maharaj noted that Caribbean governments are frequently motivated to take the legislative step with an international and regional push; the Council of CARICOM meeting agreed in 2018 to a Single ICT Space including harmonised data protection legislation - because of international treaty obligations. Countries also have international obligations via trade agreements; e-transactions, data

protection, privacy and telecommunications were cited as examples. All parties to the EPA have drafted data protection legislation, but have reserved special areas because they haven't fully implemented, but there is a timeline for implementation. Moreover, the region would likely be guided by international imperatives such as GDPR.

## **Implementing Existing Legislation**

**Question from Moderator: The Data Protection Act appeared long before GDPR, but why aren't the wheels turning towards implementation?**

Mr. Morgan offered the view that, in the Caribbean context, even those countries who have passed data protection laws, have no entities with teeth to enforce them, such as a data commissioner, and therefore **no actual enforcement is taking place** - no Data Protection Authorities have been appointed, and he strongly suspected that funding issues are holding back implementation and enforcement. Further, he said that funding for such authorities must be allocated within a framework that maintains the authorities' independence - so far Caribbean countries only have legislation to 'tick a box' for their international obligations - but they aren't as far along as they appear to be on paper because of a lack of funding.

**Question from Moderator: How have other countries funded implementation?**

Dr. Wu noted that California just passed the Consumer Privacy Act in 2018 and that perhaps data protection legislation may simply be too early for the Caribbean. He observed that regulation makes it difficult for companies to do business, especially for small businesses. He suggested that countries implement just enough regulation to ensure that companies meet GDPR requirements, so that a framework already exists for the region, with no need to reinvent the wheel.

**Question from Moderator: How is Microsoft going to support these implementation efforts?**

Mr. Mohammed pointed to the fact that there is no consensus among governments on these issues. As an example, while some governments such as Antigua and Barbuda are in support of storing their data in the cloud, others say data must be sovereign. Therefore, first there is a need to agree on guiding principles - the conversations have not reached a maturity level where the respective

governments can sign something together. In the context of Microsoft, if any customer wants to or needs to comply with data protection regulations, the company will facilitate their requests. Moreover, Microsoft supports the Paris Call for Trust and Security in Cyberspace and has been writing to governments in the Caribbean asking whether they would sign on to it, but responses haven't been enthusiastic. With regard to enforcement: if countries sign on to agreements individually, we lose the collective muscle to enforce; one can only use sanctions if you have the muscle, and individual countries in the Caribbean arguably do not. If we don't do it collectively, banning a company from one country isn't that strong relative to the entire region.

## Q&A

**Question from Kwesi Prescod, Prescod and Associates: How do structural issues of governance in CARICOM, e.g. non-binding agreements and lack of unified judicial structures - impact CDPR? These problems seem larger than CDPR. Do we have the appropriate culture of corporate enforcement? What are the next steps to deal with governance and corporate enforcement questions?**

**YW:** What is the purpose of CDPR? There is already too much regulation in Trinidad, and they're never properly implemented; we should instead try to promote business in the region - it is important for international companies to have clear rules to work with.

**VM:** Next steps include, a regional CARICOM business group. Funding is an issue to be addressed. Once this is done, the next steps should include DPA establishment, training, and populating the authorities with strong staff. A different policy approach can be taken with respect to cloud and data protection. Even in current regional legislation, some countries' laws require mandatory disclosure and some don't, some allow cross border flows of data. Regional bodies (CARICOM, CTU) should put forward core principles; there is a need for uniformity of form with respect to data protection principles.

**BM:** If you're in business, you have to be compliance with GDPR; **but the fundamentals of good data protection do not change**; using GDPR as the baseline for an organisation is a high watermark so CDPR doesn't necessarily become onerous. Why hasn't it worked in the past? It seems that the 'Copy and paste' method doesn't work. It is not necessarily a bad thing to have our own versions to deal with local and cultural nuances. Either approach (Treaty or Model) has its benefits.

**YW:** Without CDPR, there's no barrier to the market - why does every country want a say in standardisation? **Because they can set the tone for the market.**

**Comment from Rishi Maharaj:** GDPR arose in the context of the history of government surveillance, greater user sensitivity to data and privacy. There is a need to understand Caribbean context and nuance, what people are willing to share, and businesses need to understand the dollar value of privacy. He doesn't support the 'cut and paste' approach. Moreover, we have to be aware of the US CLOUD Act and its subversion of national DPRs.

**DM:** Insurance data is held in a local company's data centre that doesn't deal with Europe and doesn't need to be GDPR compliant. Yet it is still sensitive data, so we need to have rules for how those companies store our data. ANSA McAfee, the Massy Group, etc. are regional but not in the EU. Microsoft would support CDPR because they need rules to operate in.

**VM:** CDPR would be a plus, not a barrier - it would build confidence that there is a unity of legislation and approach. Within the Caribbean, with fragmented legislation and void of legislation, investors are apprehensive - how do they get customers to trust them? Comparable standards are necessary - if countries don't meet the benchmarks of other countries it poses a barrier to other countries and companies dealing with them.

**YW:** Regulation scares companies away. In East Asia, countries don't regulate until the industries are mature. The Caribbean approach appears to be 'regulate first', then nothing happens in terms of industry development.

**Question from a Naparima College Student:** The definition of 'trust' includes transparency, privacy and control. It depends on opinions, but to trust also includes obligations, not just to users but also

**to country one is operating in - how does industry tread the space between user protection and meeting the requirements of government?**

**DM:** Microsoft is a global company. Because of the sheer scale of cloud technology and its Software as a Service (SaaS) offerings, it can't customise every solution it offers, because that limits scale. Where trust is concerned, there's nobody who disagrees with pillars of trust set out - Microsoft is confident that those pillars mean they can meet legislative obligations, and they should. **The requirements of CDPR are probably going to be very similar to GDPR, but we do need them because we have regional companies.**

**Question from Glenn McKnight, ISOC Trustee: What is the cost to the local economy of not complying?**

**DM:** If a bank is ignoring any rules set out, it is costly, but it is cheaper than compliance with GDPR for example. The cost of being able to disclose a breach within 72 hours, requires technology, skills, and knowledge; **there could be companies that have been breached and have not told users, and that's really dangerous.**

**Question from Glenn McKnight: Policy without actions will not work. Where do the political will and funding come from?**

**GG:** There must also be public pressure and activism.

**VM:** There are many proactive societies, eg. those in the EU; many governments are reactive to popular drive and needs, and that's what's going to influence politics. Governments are moving towards DP laws, Cybercrime and Cybersecurity laws, using a light touch approach; but even in the regional discourse, you find CTU, CARICOM, CARICAD are all bringing discussion as a priority into the space.

**Question from Ajmal Nazir, Entrepreneur, Green Dot and Director, TT MAG: CDPR is a necessary evil but there are negative aspects of data protection. Established companies support regulations that make it harder for new companies to come into the market. Entrepreneurs don't favour**

regulation. Blockchain enthusiasts are attracted to light touch, low regulation destinations (Singapore, Malta). Regulation slows things down. Enforcement makes it difficult to get things done (days turn into months).

**Lasana Murray:** Regulation is premature. It will create a line where new firms have to invest to comply, what's more needed is best practice, we have many people playing with stuff they don't understand; IT teams are overwhelmed with people playing multiple roles, and no control over what's going on - companies have responsibilities with or without regulation; some companies are bamboozled by complexity and are abandoning information management systems and going back to spreadsheets.

**YW:** We do need legislation, and that encourages best practices, which don't specify what best practice or standard is used, e.g. ISO 27001; best practices are not laws.

**Question from a Holy Faith Convent Student: How do we turn towards proactive governments?**

**DM:** In the Caribbean, we currently have reactive governments due to not having a driver or motivator; there is an economic motive in building trust in doing business (e.g. Microsoft); if governments see money in enforcing trust, they will become proactive.

**Where should Caribbean companies store data?**

**YW:** Store data in Trinidad, the centre of Caribbean technology.

**BM:** It depends on the type of data; if it is sensitive local data, it should be localised; **major operators are regional operators operating regionally**; it would be very inefficient to have many data localisation laws, and may be more efficient for businesses to have regional localisation strategy, governed by the same CDPR.

**DM:** Not all data is the same; some is public data, some is classified data. Microsoft offers a hybrid model (data centre plus public cloud) to treat with these situations.

**VM:** It's a balancing exercise. Government is the largest custodian of data, and therefore governments are often apprehensive to have data stored anywhere else.

Section 36 of data protection legislation in T&T states that data must be stored in T&T unless the other country in which the data is stored has comparable data protection standards. CDPR requires common understanding to be in alignment with what is proposed even in GDPR.

**Comment from Albert Daniels, ICANN: On May 25, 2018, ICANN was forced to take immediate action because of GDPR entry into force. Information regarding domain name registrations and expedited policy development process can be used as a model, and ICANN's report on how it dealt with the matter will be released in February 2019.**

## **Conclusion**

Mr. Gobin closed the panel by offering a summary of the discussion, emphasising data protection and the balance between business concerns about encouraging investment, technological concerns about compliance and cost, and the privacy and security needs of users and the public. Governments have a duty to appoint DPAs to enforce existing legislation. He closed by noting, with a joke, that many companies in the Caribbean have been already been hacked: "50% have been hacked and 50% don't know they've been hacked!"

## Panel Session 2: Cultural Factors in the Caribbean Affecting Trust & Privacy for Digital Security



Cultural Factors in the Caribbean Affecting Trust & Privacy for Digital Security panel (L to R): Ms. Jacqueline Morris (moderator), Mr. Anselm Charles, Mr. Bartlett Morgan, Mr. Randall De Freitas, and Mr. Michael Walcott.

### **Moderator**

Ms. Jacqueline Morris – Former Director, TT MAG

### **Panellists**

Mr. Randall De Freitas – Manager, Technology Risk, Ernst & Young Services Limited

Mr. Anselm Charles – ICT Manager, Caribbean Community Implementation Agency for Crime and Security

Mr. Michael Walcott – Senior Manager, Operational Risk, Republic Bank Limited

## Introduction

Ms. Morris introduced the discussion with a common saying that states “in information security, users are the weakest link.” She questioned the panel whether there are certain factors that predispose users to this behaviour or perhaps there is something in our DNA that makes us more open to trusting people and having negative practices concerning digital security. She gave a reference that states that human error is a significant factor in digital security weakness, giving an example of a study where suspicious emails were used to determine how users deal with such threats. It was seen that people would open emails, forward them, download harmful links, provided sensitive information and ran executable files. This showed the lack of awareness and common knowledge on technological security. She also stated that user want security and flexibility and finding the balance between the two is a challenging task.

## Discussion

In response to the question presented by Mr. Morris, Mr. De Freitas responded by saying that culture is difficult to discuss as you have to be the object and the subject and the previous panel used terms such as reactive and proactive. Our cyber security and security awareness are a bit behind. With fraud, the effort taken to engage in fraudulent activities is minimal and some people may not know they are engaging in that practice. Mr. De Freitas then posed the question, “Do Caribbean societies increase the risk of fraud because of the trust people have within each other?”

Ms. Morris then asked Mr. Charles to share his thoughts on whether it is a Caribbean thing or just a “thing”, or maybe something that happens to younger societies in general. Mr. Charles said it’s a problem across the board, it varies from territory to territory and differs over cultures and generations. Different generations are more open with sharing of personal passwords etc. We can train our users to use any system and about the best policies without taking into consideration the day to day practices of the user. Culture comes into play when users allow trust in their peers. We need to understand the user to build more secure systems.

Mr. Walcott then added by saying, culture does make a difference, more so organizational culture than actual culture within a country. The business support etc., makes a huge difference compared to

how people act. Younger people are more open with information, middle-aged are warier and the older generations are also open to sharing information. The user is your weakest link and strongest ally. Training of users to give support across a variety of areas, but spending as much time as possible to make a system more error-proof by using biometrics, intelligent systems, etc. Also put the technology in place to protect them and yourself.

Ms. Morris said, we have been talking about ways to change the culture of users within an organization to move more towards a culture that supports security. Mr. Walcott responded, yes, you continue to do that and make it official your number 1 priority but unofficially, your number 1 priority is to ensure the correct thing is done.

Mr. Charles then said, we cannot split it into two parts, we can spend money on infrastructure and technology but we cannot forsake the education of the users. The harder you make a system for the user, there is a greater chance of the user finding a way to circum-navigate the system. Spend resources to help users understand and have a security-minded culture and make them understand it is a benefit to them as people and society.

Mr. De Freitas said, a lot of the technology used comes from western societies, their values and practices are built into the systems. There are certain assumptions built when this hits a company and certain practices and ways people are going to adopt. Mr. De Freitas then makes a statement, "Policies are just a piece of paper, and we know how to do things the right way." Mr. De Freitas then asks, "Is that a cultural practice?"

Ms. Morris asked, "How pervasive is low security culture in the Caribbean?" Mr. Walcott responded that it is not low security, but the understanding of security. For example, using the same password in different platforms that are secure and not secure. There hasn't been an issue large enough to compel the government to take that step to push cyber security forward. The political will is not there and this may be part of our cultural reasoning.

Ms. Morris gave an example which said, if people lose their money, they get it back from the bank so it isn't something that truly harmed them. Mr. Walcott said, people are affected and traumatised by it but it is observed that people still make mistakes and even the same people may continue with the

same practices. In some cases, the bank is blamed and in others, users accept that it was their mistake. Facial recognition, voice activation, fingerprint, use technology to help the users to avoid the problem.

Ms. Morris asked, what is the difference between older and younger folks? We have seen millennials are more open with sharing compared to the older folks. Mr. Walcott says, from the statistics in the bank, we see the younger and older people sharing more information and things are in place to help manage things. Mr. De Freitas said, training for practices should be a larger budget for different islands, based on the repetitive behaviour seen in certain countries.

Mr. Walcott said, it was noticed that money can be spent on training but you have to be aware of how you spend that money. Looking at the specific groupings and their attractions. Understand your different target markets and how to train accordingly. Mr. Charles said, it was realised that peers play an important role in this. In each target audience, it is better to find someone in that age/social status/range to support or push the message. Understand that the users are important.

Ms. Morris said, people developing software for us but do not understand the Caribbean people, their activities and practices. Is that something that we have been thinking about or working on in the Caribbean? Mr. De Freitas said, it is a criticism of his that when software from a western region is taken and tried to be adopted rather than adapted, then we would get the wrong results. It fails because the practices from the country of origin are embedded in the software. It is a problem that has not been addressed. The assumptions made by the developers are that of another country.

Ms. Morris asked, is it because they bring the practices of another generation that we need to use different approaches in software? Mr. De Freitas said, the younger generations prefer shorter amounts of time whilst the older generation would be able to sit for longer times to hear about the topic. This goes back to security in the form of software. Is the software produced being targeted to all generations? So, it could be a factor that affects how effective solutions are. Mr. Charles said, we fail to sit and look at the fact that our nuances are not catered for in software development. Software developers have to be aware of how users in a certain location work to ensure that users are properly catered for and their interaction with the system is secure. This applies to policies as well. We take an

information security policy and try to implement it without understanding our organizational culture. This then causes a number of human factor issues.

## Q&A

**Jarryon Paul, Entrepreneur: How does one approach building and understanding software applications for Caribbean users, how to build trust in the system for the benefit of the user?**

MW: It depends on the type of user. I do not recommend placing too much of a burden on the user.

RD: it relates to both the legislative and regulatory environments you are building it within. It needs to treat both aspects. There are two sides, the first being if the governments are interested in providing an environment for it. If you shop with amazon, etc, you have confidence because the States have the proper legislations. The second is on the developer, to market themselves and what they have done properly.

AC: know your user, know how to build confidence in specific users targeting various ages, how to target them and what is most important to them. Tailor the user experience for them without compromising security.

**Denille Charles: There is a disconnect between the adoption of technology and the adoption of security policies. We were behind on the technological train and trying to catch up has allowed security to not be at the forefront of everyone's mind. Culture is the opposite of what was said generation wise. The older folks are hard pressed to trust newer technology. How do we get them to trust this new technology?**

JM: The question can be summarised as: access to technology comes before we are prepared for it.

AC: If we had time to prepare for every advancement of technology, we would be stagnant, because it changes so much. He agrees with the age factor, personally with cloud discussions, the feedback is negative. It comes back to understanding the user, you need to understand the specific fears of a

certain age group and address them. You have to sell the benefits of embracing technology while addressing their concerns. Upgrading is not to make a better system, it is about upgrading to make secure systems. It ensures that if the user makes an error, the system is still secure. In summary, it is about understanding the user.

MW: Do not discount the concerns of the people you are dealing with, especially since the older age groups are in charge and have a lot of influence on a company. It is a matter of understanding where the risk lies, how you can mitigate it. For the ones that cannot be mitigated, think about how you will address those.

JM: Resistance to changes is not always bad.

**Youth: Do you believe the social institutions are moulded by the individual or vice versa. Do we need to “Caribbeanise” our approach on the internet and information system?**

RD: I think it depends on the culture of the society we are in. In the Caribbean, we do not have a bottom up approach, while people may do various things, they come together meaningfully to demanding something. So in my view, things are driven from the top down. People are driven by global norms and practices, where the top down management is seen.

AC: I agree that it is top down, I think it should be a bit of both. The best systems are a mix of all the systems. There are times when the individual needs to shape the institution or vice versa. There is a need to “Caribbeanise” in some instances, but do not water it down just because of where we are at. “Caribbeanise” means to understand the nuances of the Caribbean as well as keeping the standards of what you are trying to implement.

MW: People are people and each region would have their own cultures and challenges, but it is up to us to use what we have advantageously.

RD: we need to do more research in the Caribbean to guide policy.

**Hassan Voyeau, YouTube chat – Thoughts on having a national or organizational digital security survey. What are the upsides of cultural disposition?**

**Kerron Ramganesch, YouTube Chat – How do we approach the level of Standardization vs Customization of digital security policies which applied across the Caribbean jurisdiction given varied cultures?**

AC: Answer to the first question: We suffer from a lack of study in the region, any method to study our social environment is welcomed. Answer to the second question, upsides: Caribbean people are very sceptical, a large percentage of people don't believe things, fishing e.g. Most people would second guess or get a second opinion. We shouldn't look at culture as good or bad. This is the environment in which we operate, this is what influences how we do things and that must be kept in mind because it may be something we need to keep or change. Answer to the second question: Customization – never customize to the point where you lose the original functionality or security. Capture and secure those nuances.

MW: Answer to the second question: Advantages- Creativity, since we often find ways to solve issues people often grapple with. Customization comes with a cost, in terms of support, grades etc as well as training users. Make customizations based on laws practices etc.

Survey - Yes. And the questions would need to be different based on the country.

RD: Yes, more studies and data. Adapt and not adopt based on what your specific area.

Customization vs Standardization – Microsoft has more of a standardization approach with respect to the cloud and that supports sales in software.

**Glen McKnight, Live feed: How do you incorporate cultural indicators in the planning stages without compromising the local sensibilities?**

AC: How we overcame that challenge, have a chat with your local stakeholders. Understand your users and their culture. We should not force technologies on people without understanding the individual.

RD: Understand of self (individual organisation/society) the gap is understanding yourself first and then start to embed certain things without disrupting the local atmosphere.

MW: If we can agree on the result we can agree on a method and then implement.

JM: Culture and people must be considered in the planning process. It could result in the failure of a project if it is not done.

**Kish Mitchell: Education and giving awareness of not sharing passwords etc, a lot of people are not inclined to technology. How to encourage and then implement education of security?**

AC: For those who are not tech savvy, meet them where they are (older folks). People need to understand their banking information alone is not the only thing to secure. Security is a mind set and applies to everyday life, the design of sensitization and knowing your target audience will help with security.

**Kish Mitchell: How do you reach them where they are?**

AC: Go “old school”, go meet them in person, print a pamphlet and engage the community. Know who you are dealing with. I would do data collection, then design a program geared towards them. Radio, Tv advertisements, Set up a booth at a shop. Understand who you’re dealing with.

**Inflexibility. Systems can be implemented to discourage persons from sharing passwords. Authentication messages, procedures, call, email, etc. Look toward investing to find people locally who can provide solutions and be dependable supply these solutions.**

MW: We do have a local content policy on small things. But large scale would be a challenge due to the risks.

RD: To address Ms. Kish Mitchell question. There should be a social responsibility to make sure that who is using their service is aware of good practices.

AC: I agree we need to develop our local pool etc. In developing the local pool, you also need to develop the environment in which they operate by giving them the tools and training etc. With the inflexibility issue, companies are developing technology that allows flexibility without devaluing security.

## **Conclusion**

AC: It is a 50-50 with users and technology, we need to focus on both otherwise we would have issues.

RD: In closing, the internet is everywhere. I think it is good that scepticism is a thing and risk conscience is critical.

MW: As a region we need to come together to see what are our issues: legislation, education and using technology that is there.

## Panel Session 3: Using Technology to Increase Trust in Public Institutions



**Moderator :** Glenn McKnight, Secretariat, the North American Regional At-Large Organization (NARALO)

**Panellists:** Charles Bobb-Semple - Deputy CEO, The National Information and Communication Technology Company Limited (iGovtt)

Master Christie-Anne Morris-Alleyne - Court Executive Administrator, the Judiciary of the Republic of Trinidad and Tobago

Rishi Maharaj - Executive Director, EquiGov Institute

### Introduction

The third panel session instigated with the moderator, Mr. Glenn McKnight, introducing himself and giving a brief history of some technological projects he worked on such as the Baygin Windup Radio and InkMedia first Netbook computers.

Mr. McKnight introduced the topic of discussion by stating that according to OECD (2014), trust in public institutions is defined as "... confidence in the actions of these institutions to do what is right and perceived to be fair." He persisted with saying that in countries across the globe, under regimes of all types, such institutions are facing an everyday decrease in trust from the citizens they are meant to serve, a fact that evident from subjective assessments such as opinion polls, as well as behavioural indicators like declining voter participation in democratic elections. However, the application and adaptation of technology to improve transparency (e.g. open data), accountability (e.g. issue reporting platforms), service delivery and participation (e.g. electronic voter registration), among others, can create new avenues for building these increase relationships in trust between governments and citizens. He then initiated the panel session format, whereby there would be a discussion on the benefits and limitations of such technology-enabled engagement, and potential opportunities that such practices can present for Trinidad and Tobago.

Insight was given on each of the panelists to the audiences. Master Christie-Anne Morris-Alleyne, who has the distinction as the first Court Executive Administrator of the Judiciary of Trinidad and Tobago, having first held the position from 1998-2005. She returned to this position on June 20<sup>th</sup> 2017. Prior to her return she served as a project leader of the Juvenile Court Project (JCP) and planned and implemented the Children Court of the Family and Children Division of the Supreme Court. She is an attorney of law, a professional Court Administrator and a Project Management Professional (PMP), with over 40 active years in court management, court reform and judicial reform planning, design and implementation. During her judicial career, she has served the organization in the capacity of Assistance Registrar and Marshal of the Supreme Court; Registrar and Marshal, as well as Master of the High Court. She has introduced professional and modern court administration, best practice and innovation solutions to effectively streamline operation. Master Morris-Alleyne established relationships and networks with government agencies and departments at home and abroad that are essential to achieving the Judiciary's goals. Accordingly, she is well respected both regionally and internationally.

Master Morris-Alleyne conceived and pioneered the establishment of Family Court of Trinidad and Tobago, the computerization of courts of Trinidad and Tobago and introduction of Computer-Aided

Transcription (CAT) and Court audio digital recording to the Caribbean region, among other initiatives. She was the Chairman of various committees and projects including the Trinidad and Tobago Judicial Sector Reform Project Committee, the Vision 2020 Administration of Justice Sub-Committee and the Regional UWI/USAID Caribbean Justice Improvement Project. As Vice Chair of the Judicial Review Committee, she co-authored the Gurley Report. She also held membership on various committees to create the Children's Authority and to review and amend the packages of Children's legislation. She designed the Judges' first Continuing Education Seminar, and together with the Court Administration team developed the Judicial Education Institute (JEI). She was one of a team of five colleagues who drafted the Mediation Act, was also instrumental in the drafting and implementation of the Civil Proceeding Rules 1998 and introduced the civil docket system and its management by judicial support teams. Mrs. Morris-Alleyne stated that a fun fact about her-self is that she's a mother of three.

Mr. Charles Bobb-Semple is an accomplished, results- driven professional with notable success directing and project leading a board range of corporate ICT systems initiatives. With more than nineteen years of ICT experience, Charles is a certified project management professional who acquired two Masters degrees, an MBA in Business and an MSc in Computer Science. Mr. Bobb-Semple has a distinguished career spanning organizational restructuring project management, software development, system re-engineering, database design and administration. He is passionate about the strategic implementation and use of computing technology, policies and systems and seeks to utilize this approach at iGovTT and across the Ministries, Agencies and Departments that the company serves. Fun facts about Mr. Bobb-Semple is that he's a father of two and founder of an adventure group called 'Fusion' in Trinidad and Tobago and he loves to run in the forest.

Mr. Rishi Maharaj is the holder of a BSc. and MSc. in Government from the University of the West Indies. His research paper for his MSc focuses on Curbing Corruption; A comparative examination of anticorruption agencies in Trinidad and Tobago; Hong Kong and Australia. He is currently the CEO of Disclosure Today, an award winning social governance initiative whose mission is to advance transparency, empower citizens, fight corruption and promote citizen engagement in public sector decision-making and through the utilization of civic technology. Additionally, he is the Executive Director of EquiGov Institute a Boutique Consulting and Training Firm Specializing in Data Privacy Management; Public and private sector Governance &Monitoring and Evaluation as well as a consultant with Pinaka Consulting Ltd.

With over 13 years of experience within both the Public and Civil Society he has considerable knowledge and experience of the workings of government both from an operational and policy aspect as well as a unique insight into the challenges, faced by civil society organizations trying to impact civic change. During the period 2005 to 2012, he was the Senior Officer in charge of the Freedom of Information unit. He also provided technical advice in the passage and partial proclamation of the Data Protection Act in 2011 and participated in the drafting of model Legislation on Freedom of Information and Data Protection through the International Telecommunication Union HIPCAR Project. Mr. Maharaj is a certified member of the Canadian Institute of Access and Privacy Professionals and the International Association of Privacy Professionals. Mr. Maharaj is a father of two girls and as of recent has built his first e-commerce website.

## **Experiences and Challenges with Implementing Technology**

Mr. Charles Bobb-Semple stated that for being a software developer for a lot of years he has found that not doing proper analysis to determine what has to be done to solve the problems that they are trying to solve would have no value and purpose if the problems cannot be solved. As well as not communicating properly with the stakeholders involved and the users who are required to use the system and ensuring that it functions properly. Therefore, communication and poor analysis are the main challenges.

Master Christine-Anne Morris-Alleyne, in regards to implementing technology, it has to do with acceptance orientation, especially, in a place like the judiciary. She stated the judiciary is an organisation that is steeped in tradition; therefore history is important as well as maintaining it and therefore, it is very difficult to move forward. Master Morris-Alleyne said, “When seeking to introduce something new you have to think about it very carefully and you have to think about the acceptance orientation approach and add training along with remembering that it is an organisation that has several different persons within it and several different publics.” She continued with, some of the public and customers are not necessarily what are accepted as the best in society so dealing with a wide range of people, certain aspects can make implementation difficult. Bearing in mind that the fact that the judiciary is a place where there are built in interest, what may work well for others may not for the other side so meeting everyone needs would be extremely difficult. Following Master Christine-Anne Morris-Alleyne observation on the implementation of technology, Mr. McKnight asked, “Do you think the implementation you have performed, elevated trust in the institution?” She

responded, “Yes, some most definitely have. One of the areas in which the judiciary is attested internationally is the question of public trust and confidence.” She implied that the other areas were performance management which have different categories. Additionally, saying that when a judiciary is working expeditiously they are building trust among certain people within the society but disadvantaging others consequently there is always those competing interests. So the question then is, is it trust or is it now distrust because they are harming what others need.

From a civic tech point of view Mr. Rishi Maharaj stated that the challenges that are faced in terms of lack of trust in Trinidad and Tobago when implementing technology solutions to assist individuals in getting information from government were both in citizens wanting to access the information since they are unaware of what their rights are, understanding that technology could be used as a means to question the public institutions and be capable to hold them accountable for their action moreover there is a lack of buying and trust. However, from a public institution point of view, he said, “Not only in Trinidad and Tobago but throughout the region and the world most citizens still have a lack of distrust within public institution and technology could be a way to be able to break that gap.” Nevertheless, he implied that there is still a lack of trust in the technology and implementing the technology properly with being able to bridge the gap and not only to hold government accountable but to be more transparent and having a space where society could co-create and co-implement with government institutions and public institution to solve the dilemmas.

Mr. McKnight further inquired from Mr. Maharaj about the research he had done on the three different countries (such as Trinidad, Hong Kong and Australia), if there was anything from that cross cultural comparison that indicated some higher level of trust or distrust baked within the history of those countries? He replied that most people in Trinidad and the Caribbean look at best practice. What he has realised is that not only from research he has done for his master’s project but subsequently, after he worked with the government, what needs to be understood is that there are historical and cultural scenario that you have to be aware of and understand that when implementing technology to solve issues within a country, you not only need to be aware of what happens in other countries but where your country is at in the stage of development and maybe certain things cannot be implemented.

## Successful and Unsuccessful Projects

Mr. McKnight asked the panellists about some of the high points they have encountered in terms of the projects they worked on and which were highly successful and which were unsuccessful?

Master Morris-Alleyen responded that there was one in particular. As time has gone on the court have realised how successful it was but they came to that realisation too late. It was actually the introduction of Computer Aided Transcription in Trinidad and Tobago. There were several factors that caused it to be the chaos that it was. The lesson she learnt out of it was that presuming that people wanted to be more efficient and it was important to remember that not everyone wanted to be more efficient.

As she continued handling projects later on, she has taken this lesson into account. An example is the development and implementation of the court-pay system. It is a system that some people do not like because it was efficient but it allowed the acceptance orientation to be addressed differently. Other challenges encountered were public sector and service challenges that were concerned with moving the public service in a particular way. A huge challenge with dealing with these types of implementation in a public space resulted in a smoother implementation.

Mr. Charles commented that there were some successes and a lot of fails because as expressed going through a project assuming that they want to advance certain initiatives within. For instance, E-Tax, that is a success that's advanced and going. Mr. McKnight added to the discussion in terms of the failures in all projects in an organisation there are real supporters, advocates, enthusiasts and luddites (these are individuals who were against industrial revolution and technologies). These luddites today are negative towards the implementation of innovative technology therefore causes blockages when implementing a solution.

Mr. Maharaj contributed by implying that in two projects he was part of used technology to boost and improved the efficiency. In one of the projects which was the pension plan process there were some individuals who did not want to be efficient as well as there are those persons who came up with regulations and laws therefore, having to follow these rules causes delay in the process.

Master Christine-Anne said that, "A challenge that is thrown at you is not law but policies and long standing procedures." She also implied that there is a failure to recognise that law trumps policies and

long standing procedures. More often the law is not the problem, but rather the old traditions of doing things.

## **Trust**

Mr. Glenn McKnight commented saying, “Estonia is a county that has e-democracy, e-government and many of the e-procurement strategies how did they do it and why cannot Trinidad be a shining star like Estonia?”

Master Morris-Alleyne stated that in Estonia generally it is a cultural thing and there is a level of trust. Therefore, there is an understanding and an element of trust and a belief that citizens are taken care of and the system will work. Unfortunately, culturally in the Caribbean we do not have that level of trust and that affects the Caribbean greatly in terms of what can and cannot be done.

Continuing with from a judiciary perspective, transparency by large, usually presumed that it helps with public trust and confidence. However, when talking about government, authority, trust and belief in authority there is an intangible that we are not honest about and that intangible is that in order to have that trust and belief in authority there is a certain level of familiarity that is needed. Whereby, Estonia has a history that cannot be ignored and that is a history that has given it a certain kind of belief, fair and respect in authority and that is not so in Trinidad history.

## **Getting Politicians and Bureaucrats on Board**

Mr. Charles stated that since he is involved with technology, putting the infrastructure in place is something that has been done but people trump technology. He said that, “Technology is never the problem.” He stated that the issues that are needed to be addressed in terms of governance is not necessarily the ICT but as individuals both in the private and public sector because we do not have trust in each other.

## **Implementation that Enhanced Public Trust**

Mr. Charles Bobb-Semple response was by monitoring the launch of the live chat facility which led to the realisation that there was a higher usage than the walk-in facilities. It was seen as positive as it meant the country was advancing. His wish list was that he wants the payment facility, which persons could pay online without the chaos of going somewhere to get business conducted as well as moving

into an environment where all procurements are done electronically which would open the market to multiple vendors, open up transparency as well as improve performance.

Master Morris-Alleyne responded that the one that increased public trust and confidence is Computer Aided Transcription. In the court the level of trust that both sides have is the accuracy of the records. In terms of the desire of what she wants to see is an online alternative to dispute resolutions in small claims matters, the challenge is that the country is disorganised and what it cost to serve people is expensive. She referred to the example of Todds road, the amount of failed or inaccurate processes is described as a loss of money and opportunities. She desires that we can do more online litigation and mediation for small claims matter; it is something they have and want to do. Mrs. Rishi Maharaj made reference to the electronic birth paper and that the time it previously took as compared to now has dramatically decreased as other services depend on it and it impacted other sectors of the government he also mentioned that in this process there were some difficulties with others when it came to co-operating. His desire is that the civil society and government work together to actively monitor successes in projects as well as failures to assess where these failures can be improved.

## **Q&A**

**How did you get the public to begin using the court-pay systems especially, those who were preferred not to use such system what worked and what did not?**

**Master Morris-Alleyne** - responded by saying it was a combination of two things; one part being asking judicial officers to explain the process to the litigants and seeking their interest in using it which was important and worked quite well however, it was not the only thing that helped. She also described it as being traumatic since it was a trust and confidence issue. The other part was that they also kept open feedback between court and litigants. Taking away the inefficiency and making it transparent it made a different.

**What was the difference before and after court-pay?**

**Master Morris-Alleyne** - the difference was an increase in timely payments. There was approximately 40% failure to pay on time to less than 1% failure to pay on time.

**Question from the online audience with reference to The Element World Trust Index website “but people are encountering blocks in a quest for facts with 73% worry about fake news being used as a**

weapon.” We should work together to get Trinidad and Tobago rap on this index. What are your (panellists) thoughts on contouring fake news?

**Mr.Rishi Maharaj** - the response was that the government needs to be more proactive and also release information in a timely and accurate manner due to the fact that social media platforms have the ability to make fake news seem real and so when the accurate information is released it is now seen as false.

**How do you market your technological products and services, your ICT to your users and is it as a technology or a business solution?**

**Mr.Charles Bobb-Semple** - stated that there is a consulting unit comprised of five individuals who would go and find out from the ministries and understand what their plans are, what they are working on and they can assist. Next part is the citizens in terms of what is available via TTconnect in terms of taxes and they can chat online. We have not been as good in communicating with the public with what is available in any broadcast format. The representing ministries deal with advertising to the public. At iGovtt with making the processes happen.

**Can you identify two technologies that are out there in the global space that we have not yet implemented that could be a great impact?**

**Mr.Charles Bobb-Semple** - classified it as e-democracy and interact-ability as we are supposed to have a single source of truth when we put a platform on top and search we are supposed to get all information from all ministries and demographics. Next is e-democracy if you see an issue you can report it where someone will respond and there are also analytics of how that ministry is performing and how long it took.

**Mr. Rishi Maharaj** - identified blockchain and what blockchain allows. He stated that he thinks blockchain represents the net of the future. Along with the avenues that blockchain can be used to improve governance system.

# Open Forum





**Tracy Hackshaw:** Does the GDPR affect non-profit organisation and how so? How does a non-profit organisation prepare GDPR?

**Ajmal:** without knowing the mechanics of GDPR, non-profit organizations should not be exempted from the normal rules a private company would have to adhere to.

**Bartlett Morgan:** Non-profit organizations have to take a practical it has to take on board in terms of considering the longevity of the organization and the degree to which processing personal data is a significant part of what the non-profit organization does. In terms of the risk profile, NGOs has to pay more attention to it and has to consider getting more resources into putting systems in place to manage the data effectively.

**Albert Daniels:** What happens in the global community could and would affect the local environment. Caribbean countries need to follow the happenings, pay attention to situations where there are opportunities and participate in policy development in inputs because when inputs are not made into the global processes, Caribbean countries are greatly affected.

GDPR will have a significant impact on how the Caribbean communities function as the as legislation was put into place by European Union where many organizations had no choice to ensure that they were compliant and it is gradually filtering into the Caribbean territories. From a Caribbean perspective, we should always be vigilant to what is happening in the global environment.

**Tracy Hackshaw:** We need to understand how GDPR affects everyone but more importantly there is a need to understand how it affects us as Caribbean Community.

**Dev:** The GDPR forces us to think about how we treat with European data and non-European data and harmonize your approach to all data.

**Patrick Hosein:** GDPR has caused us to redact person's contact information.

**Nigel Cassimire:** What is the jurisdiction boundary for this enforcement and the consequence to businesses given they would provide all the information they used to? Can a DPA in Europe take sanctions against a registry in Trinidad and Tobago? Is that outside of their jurisdiction?

**Bartlett:** Countries outside the European Union are moved by fear in response to GDPR and its perceived impact. It is based on the business and the business model and if they are targeting Europeans. If the target is for Europeans, then as a business, it would directly impact you, and you have to comply to GDPR but if the target market is non-Europeans, then the GDPR and its scope does not apply to your operations. The focus should be on implementing good best practices if a company processes lots of data as part of the business model.

**Kevon Swift:** European DPA's are looking at ways to create to compliance club whereby they are looking to enforce through other agencies and means.

**Albert Daniels:** On the 25 May 2018, the way data was made available in the WHOIS was changed as a result of the requirements of. Expedited Policy Development Process (EPDP) was put in place to fast track what the ICANN global community's position should be with regards to DNS data that is kept in the WHOIS.

**Remote Q. 50Lindsey:** Question - In Trinidad healthcare can be a nightmare, would you agree that using technology to better communicate patient care among hospitals, nursing homes and pharmacies can help solve this? Question 2 - What challenges other than interoperability, security and privacy that needs to be addressed?

**Rochard:** The technology is initiated in Mount Hope with patients history, pharmacology inputs, however the other hospitals are not as technologized and synced as Mount Hope. Each patient has to be assigned a code pin, and going back to reference a patient's history can be temporarily stymied or

non-symptomatic and within 4-5 years problems can occur and as such a larger computer recording system is needed.

**Tracy Hackshaw:** The region suffers from the lack of data classification policies and standardization eg. date format on health records, people records, land records, etc. Reaching interoperability is always going to be a problem because there is a lack of policy and standardization across the board and there would be a need to classify data in terms of what is secured, secret and open. In essence, each ministry stores data differently.

**Patrick Hosein:** Information is not amongst hospitals and a project is being done to look at having a centralized database where data would be collected from different hospitals and you can go there to retrieve it. The problem that occurred was that different hospitals and health centres were using different systems and vendors and to put in place that system was very difficult.

**Jacqueline:** Buy-in from individuals to allow data to be used is critical because there is medical information that leads to stigma such as abortion and HIV which negatively impacts a person life such as losing your job, lose housing, you have no money, you get put on the street and you lose the things that are important to your life. Persons may perpetuate hate crimes against you. The problem is who gets access, what they get access to and our ethics regarding the patient's confidential information. Technology is not going to prevent anyone from reading a person's medical history and be confidential. People being non-confidential can prevent interoperability from being adopted on a full-scale. We need to build confidential information within our culture, that we cannot be careless with data because at times there are serious implications.

**Kevon Swift:** The Global Information Society Watch produced a report at the end of 2017 about NRIs and the report indicated that there are certain preconditions in particular, community societies that made for internet governance or NRIs to be robust and have a long-term impact on their society. There are cultural pre-conditions needed to make these changes, that is, height in sense of agency, social compact and high rise of democratic rights. Q: Where is Trinidad in terms of the preconditions and what can we do to influence systematically the environment we need to encourage digital transformation?

## Question to Youth Table

**Tracy Q:** What do you think as a young person if you were you find yourself on social media from baby to toddler?

**Naparima College:** Children are parents property until 18. Parents wish to capture the moments and offsprings recognise and have to bear this. Advice to parents to keep pictures private and share the special moments of your children.

**Holy Faith Comment:** Private social media is employed by the younger generation who have a good appreciation and knowledge of security. Youths are more aware of the technology and take umbrage to the comment that the generation is not security aware.

**Holy Faith Q:** How do we generate a culture of security and raise trust in our own ideas and products?

**Naparima College Q:** Discretionary power of government officials blocks the integration of technological solutions. Who will regulate the third parties and government official payments, especially if transactions are now electronic?

**Naparima College:** There is a need to revamp the school curriculum for critical thinking as currently, it regurgitates facts.

**Ajmal:** there is a cultural difference between the Caribbean and countries cultural view on trust. Our cultural perception of trust in the Caribbean is different from North America because of the adoption of technology and the Caribbean has not faced those issues. Caribbean countries take proactive measures against those issues without experiencing those issues.

**Tracy:** Prior to the coup attempt on July 27, 1990, people felt safe leaving their doors open, but post-1990 society changed and the issue of trust was loss in institutions, governance and in people. The lack of trust permeates online and people disassociate themselves from it to the extent where they look for trust elsewhere. The new trust is to be constructively critical. To develop a culture of trust we need to look at the new level of privacy.

**Patrick:** Few people participate in surveys with or without incentives. The problem is to develop a trust model where respondents can honestly provide information to the survey.

**Tracy Q:** Do you trust Amazon.com: Youths indicated yes and no, but they trust that it will be delivered within a particular time frame.

**Tracy Q:** Is there more trust in something like Amazon than trust in government and what they are going to do? Youths indicated yes.

**Jacqueline:** Snapchat collects information freely from the user and nothing prevents them from downloading all the information from a person's phone. People consider few information when making a decision and don't think critically about the data they share with a company or government. Trust requires deep interrogation and we need to look at that carefully.

**Naparima College Ques:** Based on the systems should be adapted instead of adopted? Should we develop our own software instead of using a foreign software based on culture? How do we develop our trust and security and make use of our developers in T&T?

**Patrick:** Companies purchase products that were designed for abroad and when applied to the local country there is a problem. The industry can produce a product just as good and even better.

**Jaryon:** In the third panel, Mr. Bobb-Semple indicated that we need something to bind us together. Are there any local initiatives/groups aimed at propelling national greatness?

**Remote Chat Ques Hassan Voyeau:** Should there be an internet hall of fame for Trinidad and Tobago?

**Patrick:** Companies purchase software that is not designed for our local environment and it is a problem in the industry. It is difficult to persuade the industry that locals can design software as good or even better than purchasing a foreign software. That has to change.

**Dev:** Open Source is an avenue for programs to be shared and allow persons to review and verify that is what it is claiming, build on the code together and tweak it to your needs

**Prof. Wu:** It will be difficult to collect data if too much attention is focused on privacy. There is a need for a balance between privacy and the sharing of data. What do you think?

**Patrick:** Locally, people do not like to share data.

**Prof Wu:** In T&T, the IT infrastructure is 15 years behind other countries. If people do not want to share data, how can we develop in terms of IoT or use this technology.

Discussions will continue on the IGF page on Facebook.

# TTIGF 2019 - Interactions



