commonwealth

DataForum'18

21 - 23 FEBRUARY 2018, **UNIVERSITY OF GIBRALTAR**, GIBRALTAR

The Data Revolution:

Maximising Opportunities and Managing Risks

Organised by

CTO

COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

Hosted by

HM Government
of Gibraltar

Event Report

Rapporteur: Commodore Ian McGhie MA FCMI Royal Navy

Consultant, Hassans International Law Firm

#CTOData

Diamond Sponsors

Gibtelecom

rockolo
A Gibtelecom Group Company

Gold Sponsors

ERICSSON

OneTrust
Privacy Management Software

Bronze Sponsor

cerillion

www.cto.int/events/upcoming-events

EXCECUTIVE SUMMARY

The agenda for Commonwealth Data Forum ’18 was notably diverse and hugely demanding. However, the conference delivered the desired results and outcomes, which reflects the high quality speakers and panels, and the diversity, eclecticism and dynamism of the delegates.

In opening the Forum, the CTO and Gibraltar Government urged everyone to exploit opportunities and tackle head-on challenges in the data space,[1] noting that education, information sharing and risk management should feature heavily in emerging solutions. Day 1 focused on two core themes of Big Data governance (legal, jurisdictional and regulatory) and the operator’s perspective, with the EU’s GDPR (General Data Protection Regulation) featuring prominently. Day 2 analysed ‘data’ in the round through the prisms of social development, protection and security, with cybersecurity bringing the conference to a close.

The size, speed and complexity of all forms of data (and associated applications) is almost too great for the human intellect to fathom, with change occurring exponentially to the extent that we may be facing a free flow of data cliff edge. The time to act is now. Countries like India are to be applauded for their ambition in attempting to capture and exploit the intrinsic value of data. The milestone GDPR legislation is almost here, but there are gaps in our individual and collective preparation that need to be plugged, noting that it will influence non-EU States data domains that are global, yet truly borderless. Its evolutionary journey should be embraced as it will shine a light on dark practices. In the context of a looming BREXIT, data divergence is neither wanted nor helpful. The nexus between Data Protection and national security needs more work to get the balance right; the arrival of 5G may expedite licencing and net neutrality solutions. Similarly, decisions are needed to determine which entities should be mandated to adhere to regulation, and those that should be subjected to voluntarily adopted standards.

The importance of stakeholder engagement cannot be over-emphasised in all areas of data, but especially in the social development arena, including tackling the digital divide. Big Data should be exploited to solve new problems (or old problems in a better way), and it should never be forgotten that data is turned into information to promote understanding, which ultimately enables our leaders to improve their decision-making. Safeguarding citizens in Data Protection terms is critically important; success here involves education, transparency and empowerment in pursuit of securing meaningful trust. Over-the-top services (OTTs) are a thorny issue that merits further – CTO led – work. Data risks are being adequately identified and captured, including the weaponisation of data by State and non-State actors (usually for the purpose of espionage or basic criminality). However (as is often the case in public and private sectors), the performance in mitigating these risks is patchy, which is not unexpected given the daunting challenges faced. We need to hold social network sites to account, but by working with them not against them, and acknowledging that they are active in areas such as child protection. Finally, the threats to cybersecurity are well known, but as it is impossible to nullify them all in short order, we should prioritise ruthlessly, with the protection of CNI (critical national infrastructure) high on the list.

[1] The term ‘data’ in the context of this Executive Summary includes and/or is indicative of: Big Data; ‘Fast Data’; Data Protection; the ‘internet of things’ (IoT); AI (artificial intelligence); and ML (machine learning).

OPENING CEREMONY

Opening remarks were made by the Master of Ceromonies, Lianne Azzopardi (Marketing and Business Development, Gibtelecom, Gibraltar), who welcomed delegates. Other participants at the Head Table for the Opening Ceremony were:

Tim Bristow (Chief Executive Officer, Gibtelecom, Gibraltar) – Key Note Address.
Paul Canessa (Chief Executive Officer, Gibraltar Regulatory Authority, Gibraltar) – Goodwill Message.
Malcolm Johnson (Deputy Secretary-General, International Telecommunication Union) – Goodwill Message *[via video-link]*.
Shola Taylor (Secretary-General, Commonwealth Telecommunications Organisation) – Secretary-General's Address.
The Honourable Sir Joseph Bossano (Minister for Economic Development, Telecommunications and the Gibraltar Savings Bank, HM Government of Gibraltar (HMGoG)) – Official Opening.

Mr Bristow welcomed all to Gibraltar, noting that hosting a CTO conference was a significant first for 'The Rock', and highlighted its undoubted strategic geo-location in the context of it being a dual gateway to both Europe/Africa and the Mediterranean/Atlantic. Mr Canessa noted the very real challenges in the data regulatory space, which graphically indicated that the data revolution was here, and that data protection should be viewed as a non-discretionary necessity, not an obstacle. Building on these themes, Mr Johnson opined that the EU Sustainable Development Goals should strive to bring technology to all, turning the digital revolution into a development revolution. Commenting on the increasing realisation of the value of data by all entities, Mr Taylor challenged the conference to define and capture this value ("……what is it?"), pointing to education and the identification and management of associated risks as being key parts of the answer. Finally, Sir Joseph Bossano urged delegates to lever on the Commonwealth's unique global reach in attempting to share and learn in all data domains. It should be used to enable a positive, collective contribution to each Member's development (noting that the concept of equality does not differentiate between big and small, rich or poor, nor male or female). In wrapping up the opening, he pointed to the fact that data has been with us for centuries, but now we were finding new ways of mining and using it, to derive generic value and improve the quality of life of our people.

SESSION ONE: MONETISING DATA

Chair: Shola Taylor (CTO). **Panelists:** David Espadas (Digital Services Director for Customer Unit, Iberia and Morocco, Ericsson); Shri O P Manhas (Director (International Relations), Department of Telecommunications, Ministry of Communication, India); Hon Sir Joseph Bossano (HMGoG); Honourable Paul Lewis (Minister of Communications, Works, Energy and Labour, Montserrat); and Honourable Vaden Williams (Minister of Home Affairs, Transportation and Communication, Turks and Caicos Islands).

Headlines: Big Data and 'Fast Data' is off-the scale in terms of quantity and speed (1 million events per million subscribers in a second) – the sky is the limit, but the time for action is now. Follow India's Big Data lead in the public domain, with the goal of "……realising minimum Government and maximum governance".

Key Themes/Points & Important Outcomes:

- Telcos engage with their clients 24/7. They need to transition from collecting data to using it to achieve profitability. Telcos collect valuable data on the customer in order to connect with them and know where to invest time, effort, money and technology.
- Customer satisfaction is a balance between expectation and experience; need a good working model of satisfaction.
- The challenges associated with Artificial Intelligence (AI) and Machine Learning (ML) clearly state the case for high fidelity Device Data Exchanges, so Telcos should place themselves in this central space (the 'vital ground'?).
- Despite the daunting size of India's data challenge (world's largest, stable democracy (1.25Bn), median age of 27 years, an aspiring middle class (250-300M), GDP growth of 7% in the last 3 years, and an economy that is expected to grow five fold in the next 20yrs), they are making tangible progress in tackling Big Data. For example, India's AADHAR (English: foundation) initiative (a unique 12-digit identity number issued to all residents, by the Unique Identification Authority of India (UIDAI), based on their biometric and demographic data) is improving lives. India's performance in the Big Data domain proved to be an impressive example of good practice.
- Need a universally agreed definition of Big Data.
- Big Data is multi-sector (industry, public health, finance, etc.), but the trick is to achieve cross-boundary coherence in pursuit of optimal derived value.
- Citizen and/or customer trust is crucial, but will only be won if they consistently see concrete, positive results in their favour.
- A dearth of experts will be an enduring problem for all CTO Members.
- A recurrent theme on Day 1 of the forum was the EU's General Data Protection Regulation (GDPR). In this session, the following points were aired:

- Noting that GDPR details are only starting to emerge, views varied on whether the framework will prove adequate or too stringent, and whether it would prove to be good for business.
- The rate of implementation will vary between CTO Members (e.g. Gibraltar with a population of 30k versus India's 1.25Bn).
- Whilst accepting the requirement for a degree of regulation, we should be not be overly prescriptive about who controls Big Data, but instead think holistically, with an emphasis on efficient information exchange and coordination, versus a stovepipes system. The goal is to achieve coherent and cogent ultimate outcomes.
- The 'centralised vs decentralised' debate proved inconclusive (e.g. distributed databases). It is difficult to decentralise in smaller countries. In reality, does centralisation actually avoid overlap and/or duplication? Harmonisation is key.
- Broad stakeholder engagement is vital (Government, Regulator, private sector and customers).
- How will non-EU Member States be policed and/or punished in terms of GDPR, especially those 'off the grid', or the likes of China and Russia?
- How will Big Data and GDPR play out for those without internet access (i.e. the 'digital divide')?
- Countries should adopt the Telco model in appointing suitably empowered Chief Data Officers (CDO). GDPR mandates Data Protection Officers (DPO).
- Can blockchain technology be used in this space?
- Legacy challenges should be considered in the context of GDPR.

SESSION TWO: GENERAL DATA PROTECTION REGULATION (GDPR) AND ITS REACH BEYOND EUROPE

Chair: Michael Nahon (Partner, Hassans International Law Firm, Gibraltar). **Panelists:** Giovanni Buttarelli (Supervisor, European Data Protection Supervisor, European Union – via video link); Ian Evans (Managing Director, OneTrust LLC, United Kingdom); Iain McDonald (Information Commissioner, Office of the Information Commissioner, Isle of Man); Paul Canessa (GRA, Gibraltar); and Alain Kapper (Senior Policy Officer (International), Information Commissioner's Office, United Kingdom).

- **Headlines: Smart Governments, Regulators and companies will embrace GDPR, as it will shine a light on dark practices. GDPR will not stymie legitimate and proportional surveillance in society. The cost of not complying with the new regulations will dwarf the costs of adequately preparing and implementing them. Data Flow remains global, irrespective of BREXIT. Europe needs an additional 33,000 DPOs by May.**

Key Themes/Points & Important Outcomes:

- Data Flows should be encouraged as it generates efficiency and choice. But need people to take more responsibility for Data Protection.

- With a launch date of 25 May, GDPR has been circa 15 years in the making. It imposes privacy by design, and its most important principles are accountability, transparency and trust. Its message to the world is that personal data is about privacy of the individual that simply must be taken seriously, and that regulation must empower individuals in the digital space.
- Data flow is global, so BREXIT will have minimal impact. BREXIT is important to Gibraltar, and the vote is a big disappointment. Believe the UK will still be a close GDPR partner. Some UK businesses will comply fully, but negotiation will occur in other circumstances.
- The GDPR's core concept is founded on the following data collection principles: lawfulness; fairness; transparency; purpose limitation; data minimisation and proportionality; data quality and accuracy; storage limitation; integrity and confidentiality; and accountability. Art 30 (Records of Processing Activities) is the spine on which other things branch off. A person's Data Subject Rights (nine in total) are established in GDPR, including 'the right': to be informed; to object; to erasure; of access to data subject; to rectification; to data portability; etc.
- Entities cannot blindly sub-contract irresponsibly (represents an abrogating of Data Protection responsibilities).
- "Don't panic"…….GDPR is an evolutionary, not revolutionary, journey. All should lever on a blueprint, conduct diligent preparation and get operationalized early, in order to create and enforce policy, with appropriate oversight. Treat GDPR implementation as a change programme, with two streams of service delivery and enabling capability (with concomitant training, IT security and funding streams). Get the gap analysis right, and secure high profile top level management buy-in.
- The predicted shortfall of DPOs should be mitigated by a mix of additional training, recruitment and contracting-out of services.
- The GDPR legal position of non-EU Member States has not yet crystalised, especially regarding accountability and/or plausible deniability. Many CTO Members are not obliged to adopt GDPR, but countries like the Isle of Man are choosing to embrace the regulations. The general consensus is that if an entity not subject to GDPR offers goods or services to an EU resident, or targets the EU market in any way, they would come under the umbrella of the GDPR framework. However, there remains a degree of uncertainty about enforcing GDPR outside the EU, noting some players (including both State and non-State actors) do not play by the rules. Similarly, what constitutes a data breach by a non-EU entity largely depends on how the relevant data was accessed; if, for example, the data was harvested via Facebook, then they might be subject to a viable legal challenge.

SESSION THREE: LEGAL AND JURISDICTIONAL ISSUES

Chair: Alberto di Felice (Senior Policy Manager for Infrastructure, Privacy and Security, DIGITALEUROPE).
Panelists: Michael Nahon (Hassans); Sue Daley (Head of Programme – Cloud, Data, Analytics and Artificial Intelligence, TechUK, United Kingdom); and Josephine Amuwa (Director, Policy Competition and Economic Analysis Department, Nigerian Communications Commission).

Headlines: Again, GDPR was writ large across this session. GDPR is a significant milestone piece of legislation in the data protection arena and, in real terms, it will have impact well beyond EU boundaries. BREXIT is less than 400 days away! Big Data divergence is not wanted, nor helpful. Are we facing a cliff edge regarding the free flow of data? As with data flow, Data Protection is borderless. It is critical that a sensible and workable balance is struck between Data Protection and national security considerations.

Key Themes/Points & Important Outcomes:

- Big Data is all about seeing and understanding the relationship within and among pieces of information, that until very recently we have generally struggled to fully grasp.
- The EU Commission's approach to Big Data is viewed through the prism of, and is part of the Digital Single Market Strategy. But distrust exists due to potential privacy risks. GDPR imposes safeguards.
- In terms of GDPR compliance, it is not enough to merely understand the legal rules; the big challenge is to get IT systems reconfigured to cope with these legal obligations.
- The UK technical sector did not want BREXIT. The prevailing views of trade members in this sector are: that a realistic and robust plan is required to ensure the UK's digital industries can thrive post-BREXIT; ensuring continued market access and regulatory certainty is of paramount importance; and a credible plan needs to be set out to ensure UK access to international talent.
- The biggest UK concern centres on ensuring data can continue to flow between the UK and EU, with legal processes in place to allow a seamless, free flow of cross-border data. It is key that the 'onward transfer' of data between countries, including non-EU countries, is done correctly.
- Faced with imminent GDPR implementation, there is a need to accurately assess whether it is part of an international movement, or not (i.e. establish segues between this new EU legislation, and extant laws and protocols). Where conflict exists, which has primacy?
- From the practitioner's perspective, guidance from regulatory authorities has been helpful, but has been unavoidably drip-fed, with inevitable changes and nuances as GDPR has crystalised.
- 60% of software tools are US; are they subject to compliance? The general consensus is that GDPR applies to every EU citizen anywhere in the world, and works on a founding principle of consent, irrespective of the specifics of a particular geo-location or situation. Also, personal Data Protection is usually enshrined as a constitutional right, which should be welcomed.
- Technology always moves faster than legislation, so in order to stand the test of time it is imperative that legal frameworks be technology neutral.

SESSION FOUR: DATA CENTRES

Chair: Graham Butler (Chairman, Bitek Global Limited, United Kingdom). **Panelists:** Danny Hook (Managing Director, Rockolo, Gibraltar); Kenva Williams (Director of Technology, Turks and Caicos Islands Telecommunications Commission); and Russell Cook (Managing Director, Sire Technologies, United Kingdom).

Headlines: Thinking about 5G tomorrow, does this dictate an end to 'net neutrality', replaced instead with structured prioritisation that reflects real world demands? How diligent are data centre operators *vis-à-vis* KYC ('know your customer')? Application of mandated regulation versus voluntarily adopted standards; which should entities be subjected to?

Key Themes/Points & Important Outcomes:

- Data centres have come a long way since their roots in 1970s computer rooms. The data centre 'journey' has included aspects such as detailed specifications, evolution to Cloud, managed services and accreditation. Benefits now include shared resources, economies of scale and energy saving, with the fundamental services being high levels of security, high integrity power and cooling, and high-end fire protection systems.
- The quality of data centres varies massively, so it is a case of 'buyer beware'.
- As 100MGb handsets become the norm in universities and hotels, should these types of organisations be licenced and/or regulated? The predominant strength of feeling is that they should not be. Regulation is good advice that should be embraced but not necessarily universally mandated, and consumer demand drives good practice in this space. However, it was noted that regulation promotes quality of service.
- Linked to the previous bullet, in considering data centres (and ISPs) as front line service entities that are most prone (targeted?) to hacking, DDOS and virus attacks, are they adequately protected? The ensuing debate coalesced around the need for regulation (the view of the 'Regulator') and/or adopting standards (the 'Operator and Consumer' view).
- ISO standards are often seen as a benchmark, but many international standards are not, or are applied with varying levels of due diligence. However, ISO standards really help in mitigating risks (hence the CTO actively promoting similar standards, such as, Cyber Essentials for cybersecurity aimed at the SME markets), but the risks can never be totally eradicated.

SESSION FIVE: THE e-GAMING INDUSTRY

Chair: Tim Bristow (Gibtelecom). **Panelists:** Phil Brear (Gibraltar Gambling Commissioner); Robert Hoskin (Group Head of Legal, Compliance and Secretariat, GVC Holdings PLC (Bwin, Party Poker), Gibraltar); and Adrian Moreno (Chief Operations Officer, Gibtelecom, Gibraltar).

Headlines: Regulation starts with the licencing process – you reap what you sow! The focus of the Regulator in Gibraltar is 'the customer first'; do operators have a culture of fairness in how they deal with their customers? The virtual circle of careful licencing ultimately makes for an easier life (in relative terms).

Key Themes/Points & Important Outcomes:

- There are circa 30 e-gaming operators in Gibraltar, but it is dynamic, with five operators currently engaged in two mergers. The 30 are split equally with respect to customer facing (B2C) and service providers (B2B). The gaming industry employs 3,500, with 1,500 in ancillary services (25% of Gibraltar's working population). The sector produces more than GBP100M for the Gibraltar Government. The e-gaming companies demand is the backbone of data services in Gibraltar.
- The remote gambling industry is a founder/building block of the Data Economy.
- The BREXIT journey is just simply unknown at present; akin to 'three dimensional chess, where the players have been blindfolded'.
- ICO ('initial currency offer'), the likes of Bitcoin and DLT ('distributed ledger technology') illustrate the complexity of issues that service providers need to manage.
- E-gaming mergers and acquisitions (M&As) pose certain challenges. Concomitant regulations are maturing, but much more data needs to be managed, secured and mapped. M&As are essentially business decisions; the Regulator should be informed of potential control changes early, with an underpinning principle of transparency.
- Data location is challenging in the e-gaming regulatory space. The current reality majors on an 'in-State' model, not particular to the EU. Stringent blocks on in-country infrastructure should be avoided. A lack of harmonisation in the e-gaming domain generates difficulties; businesses need clear rules to be communicated in plenty of time to allow adequate preparations to be made.
- The attractiveness of e-gaming is derived from it being easier to monitor and understand players hosted on the internet. This includes knowing where customers are getting their money from, noting that respectability and reputation is fundamental in this sector.
- As regards duty of care to those gambling on an individual level, the industry can be unfairly demonised. Associated analysis needs to be aggregated if fair and meaningful results are to be presented. Of 20M people studied over a three month period, only 50-70 individuals proved significantly problematic. The correct reaction when encountering these isolated cases is to apply established policies diligently.

DAY 2

SESSION SIX: BIG DATA FOR SOCIAL DEVELOPMENT

Chair: Hon Vaden Williams (Turks and Caicos Islands). **Panelists:** Jon Santos (Managing Director of Human Analytics and Africa for RemitRadar, University of Gibraltar, PhD Student); Shri Mahmood Ahmed (Joint Administrator, Universal Service Obligation Fund, Department of Telecommunications, Ministry of Communication, India); Cristina Bueti (Counsellor in Charge of the ITU-T Study Group 20 (IoT, Smart Cities and Communities), International Telecommunication Union – via video link); Abraham Kofi Astante (Administrator/Chief Executive Officer, Ghana Investment Fund for Electronic Communication); and David Espadas (Ericsson).

Headlines: Big Data aims to solve new problems or old problems in a better way. Cross-stakeholder engagement is vital. UN Sustainable Development Goals are key; they can be levered on to generate global awareness, so all should contribute to the UN agenda. Better manipulation of Big Data is improving decision-making.

Key Themes/Points & Important Outcomes:

- RemitRadar is an AI named Galileo that is capable of deep learning. It acts as an education and outreach tool; in 24 hours it reached out to 60k in triggering medical relief in poor areas of Africa. Medicine and Big Data are perhaps an unlikely and quite disparate pairing, but used effectively one can help the other.
- Big Data demands multi-fold increases in storage capacity and processing power that is able to cope with a huge variety of different data types, of which approximately 80% is unstructured. Other challenges include connectivity and capacity building (including critical mass of expertise, or the lack of it), and the need to address how to make Big Data available to all. If these issues are solved, the Big Data journey will be far smoother.
- Twitter generates 7TB of data daily, Facebook generates 10TB, and India will experience – and have to cope with – 292Bn GB of mobile traffic alone by 2019. Getting Big Data management right in India will generate a paradigm shift.
- The benefits of well-managed Big Data include: gaining a competitive edge; commercial opportunities akin to new software of the 1980s and the internet in the 1990s; facilitates customer exploitation; and represents sound risk management.
- Big Data is no longer an end in itself.
- The Ghanaian 'Coding for Kids' outreach education programme is an exemplar in innovatively bridging the digital divide.
- On a case by case basis, we should keep options open in providing increased connectivity to all (i.e. if the provision of underground fibre to rural communities would take too long, consider alternatives such as micro-wave links, power lines and/or satellite instead).
- Telcos are more likely to come onboard if the financial deltas in their Investment Appraisals are reduced. Increasing indigenous skills and capacity building (e.g. internet point of presence) is a good starting point that might make a difference and secure that otherwise elusive joint venture.

SESSION SEVEN: DATA CONTROL AND TRANSPARENCY

Chair: Hon Paul Lewis (Montserrat). **Panelists:** Rajiv Sinha (Deputy Director-General (New Technologies), Department of Telecommunications, Ministry of Communication, India); and Michele Nati (Lead Technologist), Digital Trust, United Kingdom).

Headlines: Not all information about an individual is necessarily personal information. Safeguarding must come via, *inter alia*, legislation. India is committed to empowerment, experiment and equal

access. GDPR offers innovation opportunities, including finessing the triangle of trust, trustworthiness and transparency. The Big Data nightmare is that it can be weaponised (by State and non-State actors); are Governments considering this enough?

Key Themes/Points & Important Outcomes:

- India has experienced a quantum leap in both the quantity and quality of data being generated.
- Need to get the conundrum right between balancing benefits versus personal privacy.
- The combination of 5G, Big Data, IoT (the 'internet of things'), AI and ML demands a well developed, constructed and honed Data Protection framework. The broad principles for drawing up this framework include: technology agnostic; holistic approach (including stakeholder engagement); informed consent; data minimisation; controller accountability; structured/empowered enforcement; and stiff deterrent penalties.
- 'Data ownership' is the act of having legal rights and complete control over a single piece or set of data elements. 'Data governance' is the general management of key resources.
- With nearly 450M internet users and a predicted growth rate of 7-8% per annum, India is well on the way to becoming a Digital Economy.
- In the European data market, data workers will grow from 6.16M in 2016, to 10.43M by 2020.
- More companies are embracing the digital transformation, which partially reflects a more demanding and savvy customer base. Together, the KISS principle ('keep it simple stupid') and transparency will create customer trust.
- Neither the 'lie and agree' or 'agree and forget' models of digital agreement are acceptable.
- PDRs ('Personal Data Receipts') should be human readable, and outline what has been collected in a clear and simple way. Whilst written text is understood by most, there is a place for 'icon-language' moving forwards, but this requires a degree of education.
- Deep packet data inspection should not be allowed (i.e. not the content).
- Big Data and analytics needs to be harmonised, yet remain cognisant of the individual. Again, be transparent, so that people can make an informed choice………keep the person in the loop.

SESSION EIGHT: OVER-THE-TOP SERVICES: A COMMONWEALTH STUDY

Chair: Shola Taylor, CTO). **Panelists:** Group Discussion.

Headlines: Over-the-top services (OTTs) are here to stay (voice and video), and they will continue to use 'innovative destruction'. Consumers do not want the OTTs to be licenced (relates to choice, access and price point). Despite applying appreciable pressure via intellectual rigour, even the CTO Secretary-General could not achieve consensus on licencing.

Key Themes/Points & Important Outcomes:

- Advantages of OTTs include worldwide coverage, exploitation of economies of scale, exploitation of BB connectivity, and the benefit from publicity reviews. However, it is difficult to ensure end-to-end quality control, there is less advantage of proximity, a lower capability for national dependent services, and questionable personal Data Protection and privacy.
- Australia alone receives 200 complaints every week in this space.
- Can the Commonwealth engage the OTTs?
- To formally gain the views of all Members, the CTO has produced a questionnaire for them to complete. The questionnaire targets four sector responders (Government, ISPs, OTTs and the public), with seven themes: licencing; QoS/QoE; taxes and jurisdiction; data protection and privacy; net neutrality; and interconnection. This session focused on licencing (including the plea for a 'level playing field' from the non-OTT community), and touched on QoS/QoE and net neutrality issues. In this sense, this lively session acted as a scene-setter and teed-up future, substantive engagement.
- The licencing debate in this session asked as many questions as it gave answers, but also unearthed numerous valid points (and inevitably covered aspects of QoS/QoE, taxes and jusrisdiction, and data protection and privacy):
    - Can classical or traditional licencing processes work in this domain?
    - National security is an added dimension that simply has to be considered.
    - Using a 'hammer' type approach may be a mistake.
    - Licencing to generate money is not the answer (i.e. beware mixing regulation with income generation).
    - Where do you draw the OTT line (i.e. regulating every App is impossible)?
    - When does a regulatory matter turn into a law enforcement issue?
    - Market size dictates different approaches.
- On QoS/QoE:
    - Some thought it presents a moving target, which has security and revenue generation connotations.
    - The consumer's perspective has to be factored in. For example, GDPR has been derived via widespread consultation, including with the public. After all, the consumer is the ultimate recipient of the service and/or experience.
    - Should differentiate between genuine personal use, versus business use (e.g. Skype for Business). The latter can destroy an economy, so committing to taking action represents non-discretionary activity.
    - There is a need for additional high fidelity consumer mapping.
- On net neutrality:
    - A commercial view expressed was that the reality is that 5G will force prioritisation.
    - The Indian Regulator has made recommendations on net neutrality; there will be no differentiation or discrimination of content, and traffic management will decide which critical services will not to be subject to net neutrality.
    - Fort Meade blocks 20k websites a year, for two – simplified – reasons: 'heart surgery needs to have priority over cute cat videos'; and nefarious actors have to be blocked.

- The issue is not so much blocking, but who is empowered to legitimately do the blocking.

SESSION NINE: PROTECTING THE USER ONLINE

Chair: Paul Canessa (GRA, Gibraltar). **Panelists:** Palesa Kadi (Councillor, Independent Communications Authority of South Africa); Gail Kent (Leader on Security, Global Public Policy Development, Facebook – via video link); Detective Sergeant Patricia Gonzalez (Safeguarding Team, Royal Gibraltar Police, Gibraltar); and Brenda Cuby (Managing Director, BC Training Limited, Gibraltar).

Headlines: Context and experience shapes our perspectives. Constitutional right to privacy is not an absolute right. General consensus that social network sites could do more in protecting child clients. However, detecting false details (e.g. age declaration) online is difficult, and parents could/should do more, too. Facebook presented a compelling case for the defence, and what represents 'enough action' (e.g. they currently have 10k online investigators and are recruiting 10k more).

Key Themes/Points & Important Outcomes:

- South Africa is a young democracy after a prolonged period of censorship, so feelings run strong regarding privacy.
- Social scientists say that privacy relates to an individual's human dignity, and physical, psychological and spiritual well being.
- There will be 24Bn IoT devices by 2020 – the IoT is redefining the debate about privacy issues.
- Who owns/should own information, and who controls/should control it?
- What does online protection success look like? It includes iterative, collaborative effort between at least: citizens; Governments; Regulators; manufacturers; and ICT service providers.
- 1.13Bn use Facebook daily. Each account holder can be subjected to 80+ verification questions (i.e. it is not just about a password).
- Facebook works with others and readily shares information (including data on threats), and they are passionate about developing a credible online eco system.
- Facebook counts a child as someone under 13 years of age, a criteria on which the telecommunications industry and regulators appear to have followed suit (is this legally incorrect?). Facebook verifies age via a mix of ML (gives signals about being younger), and check-pointing (age and identification verification). Removal of online information is on a case by case basis, but usually within 48 hours for straight-forward cases.
- Parental supervision and control is often impacted by a lack of computer literacy so, as ever, education is vitally important (as part of the school curriculum?).

- Protecting the user online, including the ‘right to be forgotten’ topic, plays out differently in the policing arena; serious criminal offences have no right to be forgotten.
- Dialogue is ongoing with a view to potentially wiping under-18 social network data clean when an individual becomes an adult (on request, and exempt criminal record type information).

SESSION TEN: DATA PRIVACY AND SECURITY

Chair: Palesa Kadi (Councillor, South Africa). **Panelists:** Shri M Akhya (Chief Vigilance Officer, Department of Telecommunications, Ministry of Communication, India); Alberto di Felice (DIGITALEUROPE); and Bradley Tosso (Head of Information Rights Division, Gibraltar Regulatory Authority).

Headlines: ‘Independence of the Regulator is a corner-stone of privacy’. GDPR versus boundaries of law enforcement…….there are still some unknowns. Trust levels vary massively depending on the State you live in.

Key Themes/Points & Important Outcomes:

- Data Protection refers to protecting the confidentiality, integrity and availability of any data or information.
- In India the right to privacy is protected as an intrinsic part of right of life and personal liberty.
- Telcos are audited and re-licenced annually in India, and they have established a legal framework Committee of experts to ensure coherent growth of their digital economy. Furthermore, India has set up organisations such as the NCCC (National Cyber Coordination Centre – with connected cells), a National Information Centre, and CERT-In (Indian Computer Emergency Response Team), and are proactively and aggressively driving up awareness in all facets of cyberspace.
- In the EU, layers of privacy and security have been created, including: GDPR (protection of personal data); ePrivacy (privacy in electronic communications); European Electronic Communications Code (telecommunications regulatory framework); and NIS Directive (network and information security). It is interesting that ePrivacy (personal) comes under GDPR (data protection).
- International data transfers are ‘somewhat under attack in the EU’.
- In the context of privacy and citizens rights versus broader security, we live in interesting times.
- Everyone agrees that privacy must be viewed differently when dealing with actual or potential terrorism, but some question if we can be sure, or trust that – generic – Governments (or hackers?) will consistently act responsibly and with apolitical impartiality? The truth is that the debate should not be between privacy and security, as both areas need to be satisfied, which calls for collective responsibility, collaboration and cooperation.

- Each situation is different. The emergence of technology in post-war environments is inevitably accompanied by greater suspicion and more varied sensitivities. The more responsible amongst us want to be ‘global citizens’, but what becomes of the State, and therefore individuals, when a Government is untrustworthy?

SESSION ELEVEN: CYBERSECURITY CHALLENGES

Chair: Hon Sir Joseph Bossano (HMGoG). **Panelists:** William Jackson (Vice-President, Technology Projects, Gibtelecom, Gibraltar); Spencer Thomas (Chairman, National Telecommunications Regulatory Commission, Grenada); and Alee Fa’amoe (Deputy Chief Executive Officer and Executive Director ICT, Cayman Islands Utility Regulation and Competition Office, Cayman Islands).

Headlines: There will be more than 20Bn ‘Smart’ devices by 2020 (courtesy Gartner Research). In terms of cybersecurity, the balance of power is with the ‘bad guys’. Need to prioritise the protection of CNI (‘critical national infrastructure’ – power stations, water supplies, undersea cables, etc.). State and non-State actors must be considered in this space (i.e. espionage, as well as cyber crime and anti-social and/or unethical behaviour).

<u>Key Themes/Points & Important Outcomes</u>:

- The challenge of securing networks is growing exponentially as cyber attacks grow in volume, form and complexity.
- DDOS attacks have been happening since 1974! However, they have grown from typically notable attacks of 300Gbps in 2014, to 1.2Tbps in more recent times.
- As regards the IoT, anything you buy is connected to the internet, with huge facilities but low organic capabilities (e.g. OS, memory, etc.).
- The latest Reaper BOT is just gathering hosts (2M enslaved nodes)………..what is the next step?
- Anyone can now enjoy low entry in terms of access to massive capability at low unit price.
- Attack vectors today are typically high intensity, short duration and repetitious, with escalating amplification of attacks.
- Best practice solutions are: prevention (policies and procedures, fair usage policy for users, incident response times, etc.); monitoring and alerting (reaction times in low minutes); mitigation (need tried and tested solutions); and educating customers (including their business continuity plan).
- The internet generates levels of utility rarely seen before, but also creates vulnerabilities on a similar (pandemic?) scale. A case of risk and reward, but the risks are getting bigger, and we are in reaction vice prevention mode.

- From an oversight perspective, tackling negative cyber activity requires a central pillar of a regulatory framework, and education should seek to encourage cultural, mindset and attitudinal change.
- Part of the solution lies in AI and multi-layered protection (e.g. system air gaps, built-in redundancy, smart Business Continuity plans, rapid reaction teams, etc.).
- The difficulty of attribution and plausible deniability make policing this issue extremely hard.
- Noting the obvious national security aspects of cybersecurity (i.e. non-discretionary activity), this is not an easy area of governance or commerce to conduct accurate business cost benefit analysis.
- Are Governments the right ‘champions’ in this space?
- There is a general sense that entities can cope with this challenge at a localised level, but on a global scale the cybersecurity spectre is way past daunting.

CLOSING CEREMONY

Commodore Ian McGhie Royal Navy (Retired) (Consultant Hassans International Law Firm, Gibraltar (‘*Rapporteur*’)), Sir Joe Bossano (HMGoG) and Shola Taylor (CTO).

As ‘*Rapporteur*’, Ian McGhie cantered through the highlights of the two day Commonwealth Data Forum 2018, which effectively also represented closing remarks. On completion, this left Shola Taylor to give his closing address, in which he thanked participants for their presence at a very rewarding conference, and he also expressed his gratitude to Sir Joseph Bossano and Her Majety’s Government of Gibraltar for hosting their inaugural CTO event. Sir Joseph Bossano then formally closed the Forum.

CONCLUSION

The Forum succeeded in rising to the challenges set by the CTO and HMGoG. All participants made valued contributions and derived precious insight in equal measure regarding maximising opportunities and managing risks in a data revolution that is accelerating fast.

Enduring themes emerged, including: the importance of learning from each other via rich and frequent dialogue, and information sharing; the pivotal role of education in this data space; and identifying and capturing risk, yes, but then confidently taking bold mitigating action. The latter point is especially important given the rate at which data threats and challenges are proliferating.

The dominant topic on the first day was GDPR, and social development and protecting the individual on the second. In real terms, GDPR is region agnostic; its impact will be felt by all (albeit to varying degrees) in what is a borderless global data domain. Views differ on exactly how GDPR will help or hinder in exploiting the undoubted benefits of Big Data, as well as facing-down its myriad associated challenges. However, some consensus was reached in certain sessions: the new regulation is an evolutionary journey that should be broadly welcomed; both the public and private sector are not as well prepared for GDPR as they should be; and BREXIT should not be allowed to block data flow. Turning to Day 2's social development and the rights of the individual discussions, an appreciation emerged that equilibrium between competing demands (such as Data Protection versus national security considerations) can be achieved, but delivering success on this front dictates effective, wide-ranging stakeholder engagement. Bridging the digital divide is a pivotal first step, and the symbiotic relationship between transparency and trust cannot be over-stated.

There was universal acknowledgement that the time to act in managing all aspects of data is now, but securing agreement on the various courses of action requires yet more work. This situation was graphically reflected in the debate on cybersecurity; the concomitant threats are complex and daunting, but greater commonality and joint effort is required to tackle them in a prioritised way. Similarly, OTTs remain a perennial problem in certain sectors (notably the 'regulation or standards?' debate), although ongoing CTO-led work will surely help coalesce a collectively agreed way ahead.

Finally, there was a subtle undercurrent throughout the conference relating to decision-making, particularly by the leaders of our various entities (whether they be public, private or commercially facing). Arguably, the single biggest advantage of the data revolution is that, if managed correctly, it promotes far greater levels of knowledge and understanding, which in turn should lead to better and/or more accurate decisions being taken. The slight irony is that if we fail in this space because we do not exploit data opportunities and, even worse, become overwhelmed by its challenges, then decision-making will suffer. Getting this conundrum right is key.

Overall, the Data Forum has significantly move forward CTO Member's understanding of what the data revolution means to them from the opportunity and risk perspectives. Equally significant, it highlighted pressing individual and collaborative priorities, and where inevitably limited resource should be channeled.