UK Internet Governance Forum

Report from UK-IGF - 16 June 2015

Welcome: Baroness Rennie Fritchie, Chair, Nominet & Russell Haworth, CEO, Nominet

Baroness Rennie Fritchie welcomed participants to the UK-IGF. She thanked all the committee members who helped organise the event and coordinate sessions. Special thanks were given to ICANN for sponsoring the remote participation and also to ISOC England for providing logistical support for this. Rennie outlined the programme for the day and emphasised the importance of participation in the discussions before introducing Russell Haworth, Nominet's Chief Executive.

Russell began his keynote by setting the UK-IGF discussions in context. The internet contributes to over 10% of the UK economy. This equates to £180 billion per year which is greater than the manufacturing or retail sectors. The internet economy is expected to grow to over £200 billion over the next five years, making the UK economy one of the largest internet based economies in the world.

Talking of the huge impact that the internet has on our lives, Russell referenced findings from a survey by the Boston Consulting Group in 2010. 25% of people surveyed said that they would consider giving up sex for a year in order to maintain their broadband connection. The figures for other indulgences were much higher: Some 65% would give up alcohol; 76% chocolate; and 78% coffee!

Russell stressed that a combined approach is the only way to effectively govern the internet especially as it continues to change and develop. He explained hoe the Internet of Things (IoT) is revolutionising the internet as we know it. It is estimated that 4.9 billion things will be connected to the internet by 2015, increasing to 26 billion by 2020. The IoT has a range of social and economic applications. Smart metering, assisted living and the work that Nominet is involved with on the Oxford Flood Network were highlighted as examples. This increased usage brings an increased need for digital management. Events like last week's hacking attack on the US govt personal data serve as a stark reminder of the risks.

Russell posed the question: How can we continue to embrace evolution and change while maintaining governance and security? He then explained steps that Nominet is taking to improve security. There are over 3 million domain names registered worldwide, including over 18 million in the UK, 60% of which end in .uk. Domains names need to be secure, accessible and trusted and this is a shared responsibility. As well as Nominet's dispute resolution service, it important that they work with law enforcement to help prevent exploitation. As an example of this he highlighted how over 3 thousand domains have been suspended due to a change in Nominet's terms and conditions to prevent criminality.

Nominet have also developed a product called Turning which decodes DNS traffic to identify, locate and mitigate the effects of botnets and other malware that is abusing the network infrastructure. As custodian of the UK internet Nominet use this tool every day to look at the 3 billion DNS queries that come across their servers.

Russell concluded by stressing that Nominet is a strong supporter of the multi-stakeholder model and called for participants in the UK-IGF to drive more focused internet governance initiatives at a national level. He suggested that the ultimate aim is to shape a digital world that is a good place to inhabit. Everyone should be able to learn, interact and be safe n the internet, not be threatened by it.

Plenary One: What are the major challenges and opportunities in Internet governance this year? –

Coordinated by Nominet

Panel:

- Dr Vicki Nash, Oxford Internet Institute (Moderator)
- Dr Olivier Crepin-Leblond, ISOC England
- Xianhong Hu, UNESCO
- Andrew Puddephatt, Global Partners Digital
- Philip Rushton, BT

Xianhong Hu began the session proper by drawing attention to UNESCO's 'Internet Study', a result of an 18 month stakeholder consultation (see http://www.unesco.org/new/en/internetstudy), before continuing to express a wish to secure Human Rights through Internet governance, as a new space to hold such discussions.

Olivier Crepin-Leblond followed by highlighting the deadline for the IANA transition in September 2015 as an important event on the horizon, noting that the IANA stewardship transition for the naming functions have issued a proposal for consulatation, while the accountability track was due to have a second consultation in August. It was also noted that the technical function of IANA required only nine personnel, and that it was the first practical example of a multistakeholder governance working effectively, doing so quicker than a governmental alternative.

Andrew Puddephatt began by expressing a concern about the renewal of the IGF mandate in December 2015, especially given the number of parallel discussions which attract more governmental and corporate attention. A further concern was located in the progression towards a propriotorial internet, recieved by end users through apps. Finally, a call was made for governments to develop a coherant position towards Internet legislation.

Philip Rushton re-emphasised the importance of greater coordination between Internet governance debates, praising MAGIG for its civil society engagement. There was also a request for governments to engage with thier respective UN delegates, and other channels, to ensure that the IGF mandate is renewed, thus guarding against exclusively governmental decision-making fora.

Questions and comments from the floor:

- There were some attempts not to view the UK-IGF as just a 'talk shop', but also an appreciation that the same issues have recurred for as many as ten years.
- A desire to engage the private sector was raised, particularly given their importance in issues such as data protection.
- There was consensus that civil society ought to insist on Internet governance remaining an inclusive debate.
- It was noted that there is a distinction between personal control of data, and the corporate control of personal data.

Plenary Two: Privacy and Security in the Digital Age – Coordinated by the Department for Business, Innovation & Skills

Panel:

- Rachael Bishop, Department for Business Innovation & Skills (moderator)
- David Brewer, Digital Catapult
- Abhilash Nair, Strathclyde University
- Robin Wilton, Internet Society

David Brewer opened the discussion by suggesting that there was a mandate for citizens to identify themselves, citing the UK Government's Verify identity assurance scheme as an example of how this can be actualised, highlighting in particular its private sector engagement as a 'Know Your Customer' (KYC) verification control.

Abhilash Nair followed by suggesting that sharing personal information today is not a choice but a necessity if someone wants to access services found online. He continued by suggesting that a perceived lack of trust in the Internet could be improved by all stakeholders – for instance, industry can ensure privacy by design and be transparent in the way that data is manipulated or consent obtained, while customers can ensure their rights do not end when data reaches a third party. In particular, more needs to done to ensure that consent for further processing and manipulating of personal data is not obtained by means of small print within standard terms and conditions- reasonable steps should be taken to specifically bring onerous clauses to the attention of consumers/data subjects.

Robin Wilton felt there was not a balance to be struck between privacy and security, but that both could be optimised in a mutually reinforcing way. Refuting another popular phrase, it was suggested that a trade between privacy and convenience was a trade for comparatively little weight. There was a call for policy to concentrate on knowledge protection, rather than the lower value targets of data or information protection. The potential for understanding personal identity as a mass of data, rather than retrospective identity assurance, was acknowledged.

Questions and comments from the floor:

- There was a consensus that a business model which allowed a rational move away from the status quo – from a customer either providing personal data or not being able to use a service – was a missing but requisite step for expedited commercial change.
- That there might be mileage in a traffic light system which rates data transactions, where 'green' could indicate that no data will be stored, 'orange' indicates that data will stored for company use while 'red' indicates the sharing of data or metadata with third parties.
- That it is disappointing if or when data breech notification is the main motivation for companies to meet privacy standards, but such notification can also serve to demonstrate the weight of legalisation when enforced.
- It was suggested that we ought not to expect to solve the privacy debate online since it has a long, continued history of being unresolved in the real, offline world.
- Consumer education was highlighted as an important tool to advance online privacy, but situated in context of other interventions which may be more suited to a particular point in a consumer's decision cycle.
- There was a suggestion that biometrics might not be infallibly reliable as a form of retrospective identification, since claims of the life-long reliability of iris biometrics were based on a false assumption: namely, that if the visible iris pattern is the same today as in an old photograph, the biometric is also unchanged. However, most iris biometric systems use near-infrared light, which means the resulting image is not directly comparable with a visible-light photograph.

Keynote address: Hon Ed Vaizey, Minister for Culture and the Digital Economy

Report to follow.

Three parallel workshop sessions

a) **Identity and open standards** - Coordinated by BCS

Panel:

- Louise Bennett, BCS (Moderator)
- Andy Smith, BCS
- David Williams, BCS

Louise Bennett began the discussions by referencing the BCS's Year Book and its conclusions. The full report is available at: https://policy.bcs.org/sites/policy.bcs.org/files/10%20Aspects%20of%20Identity%202014-15%20CURRENT%20FINAL.pdf.

David Williams opened by suggesting that the workshop theme could be addressed in terms of risk balance, usability and the increasing use of mobile technology: addressing risk balance, it was suggested that security methods be suitably selected depending on their location in the chain; usability in terms of simplicity was addressed by discussing different types of credentials; the advent of near field communications (NFCs) was highlighted as a possible security risk and as an environment with a lack of legal liability precedent.

Andy Smith followed, using the example of gambling website server migration to outline how a naive change in legislation – for example to improve tax income or customer protection – might in fact have negative consequences for the consumer by causing websites to move to non-EU locations and take customer data with them. This is a serious privacy and data protection risk, not least because there is a lack of cross-jurisdiction legal enforcement.
Louise Bennett spoke on behalf of John Bullard of IdenTrust (absent panel member), drawing attention to the idea that progression towards an open system (for instance EU governments and businesses using the same identity credentials), might be less useful than a closed system like a normal payments system, since issues of liability and trust are not as well attended to. Further, it was suggested that anonymous payment mechanisms might still have utility for legitimate actions.

Questions and comments from the floor:

- Age verification was discussed, particularly with regard to the retail sector and the opportunities surrounding a publically available specification (PAS) from BSI, together with the issues of parental control and costs to the retailer.
- It was noted that the BCS conceptually agree with the UK Verify scheme, but that panel members speaking personally felt that cross-reference checks, data protection and the lack of a business case were significant implementation problems that remained unresolved.
- There was a belief that strong identity markers are not necessarily easy to test, especially if, in the case of Verify, the relevant data is held outside the UK.
- That new technology might not be the solution to unique identifiers given the test case for cable authentication was 1867.
- It was suggested that the discussion be widened to consider not just personal data but the relationships between data, devices and people.
- The Annex to the EU Digital Security Act was highlighted as a future point of discussion.

b) **Explanatory session for newcomers** - Coordinated by RIPE

- Marco Hogewoning, RIPE(Presenter)

The presentation provided a high level overview of the Internet's fundamental structure, including the Domain Name System, routing and the transition of IANA stewardship. Comprehensive slides are available here.

c) **Multi-stakeholder cooperation** – Coordinated by Global Partners Digital

Panel:

- Lea Kaspar, Global Partners Digital (Moderator)
- Dominique Lazanski, GSMA
- Desiree Miloshevic, ISOC England
- Matthew Shears, CDT

Report to follow.

Nominet and the Internet of Things

Presenter: Bryan Marshall (Nominet)
Moderator: Dr Patricia Lewis (Chatham House)

The presentation focused on the lessons that Nominet had learnt from 18 months of applied research into the Internet of Things. The specific example, referred to throughout, was the Oxford Flood Network – a real world problem which Nominet chose to get involved with, in partnership with LoveHz. Setting the problem in context, it was explained that Oxford is a known flood risk area and that while the Environment Agency monitors Oxford's rivers at key points, residential flooding also occurs from back streams, which were not monitored. The proposed solution was to let residents place a wireless water level sensor over any streams within their property and use the data to create a personalised early warning system. Utilising a definition the Internet of Things as 'where the digital world meets the physical world', it was highlighted that data capture using sensors is complex and messy, requiring a level of intelligence to minimise distorted readings. The limitations of small, battery powered devices were also mentioned, together with the physical difficulties of running a powered wire to a device for constant, real time communication. Further challenges were expressed in terms the cost per unit, the risk of the unit not being securely stored and the varying range, power and data rate of different connectivity methods. One important ethic expressed was that the Internet of Things ought to democratise the problem solving process, allowing people from different disciplines to add value.

The only comment from the floor, in the timeframe available, was that perhaps the technology for the Internet of Things is already available, thus the focus should instead be on education.

Three parallel workshop sessions

a) The global fight against online child sexual abuse material - Coordinated by IWF

Panel:

- Claire Lilley, NSPCC (Moderator)
- Vic Baines, Facebook
- Dave Miles, Family Online Safety Institute (FOSI)
- Sarah Smith, Internet Watch Foundation (IWF)
- Michael Taylor, Strategic Centre for Organised Crime, UK Home Office

Vic Baines began by outlining a set of industry commitments made at the WeProtect global summit in December 2014, drawing attention to Facebook's relationships with governments, users and charities in a coordinated, cross-border effort to reduce sexual abuse material online. There was a request that some countries bring more cases to prosecution in order that there are fewer safe havens worldwide.

Dave Miles suggested that the UK was world-leading in engaging with the less mainstream issues of child sexual abuse, having progressed from cyber bulling. It was highlighted that one development of this focus was blocking search content in collaboration with Google, removing content surrounding 100'000 search terms, in 41 languages and appearing in 140 countries, leading to a 70% drop in such searches. Finally, a future challenge was identified in terms of tackling peer-to-peer networks carrying such material.

Sarah Smith began by highlighting the change in the IWF mandate to proactive search and the subsequent increase in content removed. The global nature of the problem was again mentioned – only 0.3% of the 31,000 instances of material actioned for removal by the IWF in 2014 were held on UK servers – together with the notion that an international challenge requires international support.

Michael Taylor added that the United Arab Emirates are hosting a follow up summit in November 2015, which will be focused on coordinating national responses, disseminating best practice and discussing capacity building for countries with limited resources. It was also hoped the summit might more fully engage with Latin American and Middle Eastern countries. The allocation of new funding from both the UK government and UNICEF also featured.

Questions and comments from the floor:

- There was consensus that sharing technical solutions, both between sectors and between governments, is a useful point for continued action, although debate was had about whether this was more or less important than innovation.
- It was clarified that the IWF, as an independent body, will be able to distribute a hash list between institutions and governments in the same way it currently provides a URL list of known child sexual abuse addresses.
- Age verification was discussed, especially the Facebook 13 year old age restriction.
- Two people were forthright in their challenge to social media platforms, saying they were not using technology which is used in other sectors (gambling and retail) in order to prevent and detect crime and under age users. Why not?

By way of conclusion, the panel offered their hopes for progress in two years time: these included the emergence of a single, global coordinated response; the sharing of hash technology becoming simple, best practice; preventing such material being uploaded at source; a well-funded plan for education, the existence of fewer safe havens and that we have a body of research evidence about what deters offender from looking at child abuse images in the first place.

b) Economic impact of the Internet & Mobile commerce - Coordinated by ICANN and GSMA

Panel:

- Dominique Lazanski, GSMA
- Jean-Jacques Sahel, ICANN
- Brian Williamson, Plum Consulting

Report to follow.

c) What is the "Internet of Things" and why are open standards important? - Coordinated by ISOC England

Panel:

- Benedict Addis, Web Observatory
- Dr. Nicholas Allott, nquiringminds
- Christian de Larrinaga, FirstHand
- Prof Chris Marsden, Sussex University
- Dr Thanassis Tiropanis, Southampton University
- Dr Alison Powell, LSE

Benedict Addis opened by situating Shadowserver in the context of CERT, before outlining its main operations, in particular its desire to improve the overall security of the internet by scanning and notifying organisations about vulnerable protocols in use. A demonstration, scanning for video devices utilising SNMP, was included later in the workshop.

Nicholas Allott continued, defining the Internet of Things as a device which creates content, and thus operates as a server, rather than receiving content as a client. Addressing standards and implementation, it was highlighted that many IoT devices don't support an IP stack, that security was a requisite for improving IoT uptake and that there is mileage in newer protocols such as CoAP and JSON-RPC.

Alison Powell, focusing on the consumer experience and referencing popular culture, suggested that there is currently an 'Internet of Commercial Things' which looks set to develop into an 'Internet of Broken Things'. It was noted that a device and its data is currently locked into a commercial, proprietary ecosystem with a lack of interoperability, and that the user experience is defined by frustration.

Thanassis Tiropanis discussed web observatories and its marrying of data (particularly open data), infrastructure and people. A continuum along the axes of ownership and services was offered as a way of discussing the ownership of 'Things' rather than data.

Chris Marsden began by suggesting that while the IoT has existed for 25 years, it is now more of a legislative topic since it has begun to affect more people - even if regulation will only be a small part of an overall solution, not least since it is rarely enforced. The diminished market opportunities as a result of reduced consumer trust were mentioned, together with the 'Internet of Polite Things' as a model for increased individual control – for instance by requesting consent.

Questions and comments from the floor:

- It was noted firstly that the choice to engage in IoT data capture was not just for individuals, but also for local governments with the advent of smart cities; secondly, that a recent Pew Research survey found individuals were resigned to their data being shared, rather than willing it.
- There was consensus about the importance of regulating where the customer does business.
- In terms of improving the current state of affairs, there was debate about whether 'Things' (i.e. technology) or people (i.e. consumers) must be 'fixed' first.
- Privacy regulators, including the FTC, were considered in reference to data audit, consent revocation and default standards.
- It was clarified that when vulnerabilities were identified, patching rather than blocking the port ought to be first suitable solution, although this might be more difficult with IoT.

Plenary Three: Net Neutrality & the Open Internet - Coordinated by Chatham House

Panel:

- Patricia Lewis, Chatham House (Moderator)
- Julian Ashworth, Group Industry Policy Director, BT
- Renata Avila, World Wide Web Foundation
- Dr Ian Brown, Oxford Internet Institute

The session began with Julian Ashworth offering an etymology of 'net neutrality', highlighting how its meaning might have changed from a form of negative discrimination, in terms of ISP blocking, to positive discrimination, in terms of traffic management. He suggested that competition between service providers is the driver of net neutrality and an open Internet, before clarifying the conditions under which BT might block traffic, including as a result of customer a request e.g. parental controls, where legally obliged e.g. court orders, or to prevent access to malicious content.

Renata Avila followed, praising Chile for ratifying the first net neutrality law, before outlining the challenges facing net neutrality in developing countries, including political pressures to maintain control, for example in Venezuela, together with limited access for and content from the global poor.

Ian Brown delivered a presentation on recent research - produced in collaboration with Alissa Cooper (a Phd student at OII) - which ultimately rejected the claim that consumer switching, and thus competition, is a sufficient disincentive for ISPs in discriminating between traffic. Utilising a selection of quotes collected during interviews, he continued to highlight a level of consumer confusion, ambivalence to discrimination from providers and the heightened barriers of switching broadband providers in comparison to other services.

Comments and questions from the floor:

- It was contested that the UK might be model net neutrality, or indeed that it is a competitive market.
- There is a need to clarify what constitutes a specialised service, and hence a standard channel – as yet this is not something on the EU agenda.
- There was debate surrounding whether mobile and fixed line internet should be governed collectively by broad principles, or individually and specifically.
- It was highlighted that Sky is the only UK ISP without traffic management.
- A specific, reoccurring question about why many ISPs resorted to blocking NTP port 123, which provides a timestamp function, when a vulnerability was discovered last year.