Report from the UKIGF meeting - March 2012

The Nominet Annual UK Policy Forum was held on 22 March 2012 and as part of this event the UK-IGF ran three interactive workshop sessions. The workshops were used to help develop UK-IGF messages to feed into the Internet Governance Forum 2012.

The UK Internet Governance Forum is a collaborative partnership between Nominet, the UK Department for Culture, Media & Sport, key parliamentarians and other organisations taking a leading role in making the internet a better place.

Its aim is to provide a local forum in the UK that engages industry, government, parliament, academia and civil society in debate on Internet Governance issues. As well as encouraging partnerships and coalitions that deliver solutions and demonstrate best practice for others to learn from.

Other influential stakeholder groups that are taking part include the London Internet Exchange, the Children's Charities Coalition for Internet Safety, The Internet Watch Foundation, Raceonline 2012 and Childnet.

REPORT ON UK IGF WORKSHOP 1: IDENTITY GOVERNANCE ON THE INTERNET - WHAT ARE THE ESSENTIALS?

John Bullard (Global Ambassador, IdenTrust), discussed the essentials if identity governance for e-commerce with the participants saying that there should be "no entity without identity". It was agreed that for global e-commerce to flourish it is necessary for individuals and businesses to be able to assert who they are and for that assertion to be trusted by the other party to any transaction. Interoperability in the commercial world goes well beyond questions of technology interoperability. Indeed technology itself is seldom the problem and there are a number of "Standards" bodies (e.g. OASIS, ISO & Kantara) which exist to harmonise and deliver such technology interoperability. The more difficult areas are in Legal and Policy that are also essential ingredients for true business interoperability in the underlying e-Identity framework. In e-commerce the Law of Contract is vital as it is essential for all parties to know at all times where liabilities rest. There is no need for Governments to assert identity for commercial transaction. The essential requirement is for contractual relationships to be clear at a scheme level.

Lord Merlin Erroll (Chairman of EURIM) discussed the need for proportionality between privacy and security, particularly in the relationship between the citizen and Government when services were being delivered to citizen's digitally. It was agreed that the starting point should be that privacy is good and security is good. Identity assurance schemes of necessity involve some intrusion into personal privacy. An Identity Governance Framework must, therefore, recognise that different people will, at different times, require a different balance between their individual rights and the rights they cede for the greater good. It must recognise that too little privacy is just as damaging to society and security (by enabling more criminality or chilling the democratic process) as is too much privacy (by hampering law enforcement or enabling abuse of power). And it must ensure that the benefits the Internet can bring are not stifled by an over-strict control on who can connect.

Louise Bennett (Chairman of the BCS Security Community of Expertise) examined identity governance issues to illustrate the context dependency of what is considered illegal or unacceptable activity in different societies. One example was

anonymity of social network sites. On the one hand, some parents in the UK campaign for an end to anonymity, so that their child can be less easily bullied on-line. On the other hand, activists who belong to protest groups or banned religious groups in countries with repressive regimes argue that anonymity on social network sites is essential. Similarly there are radically different views on copyright enforcement on the Internet. Copyright owners consider free distribution of their material to be theft that will stifle creativity. Those in piracy movements argue equally forcefully that this is protection of an outmoded business model. Blocking and filtering are common law enforcement responses to censorship of content and its perceived theft. It was agreed that these are blunt instruments that just drive illegal activity elsewhere. In addition DNS filtering is widely seen by those in developing countries as stigmatising the majority of legitimate users, since, at times anyone using an IP address with certain country domain names could be blocked from Financial transactions and therefore prevented from doing business on the Internet.

In addition to the above specific discussions, the workshop participants emphasised that reputation and identity are closely related and well publicised scams become associated with certain countries and reduce trust in doing business with all individuals or entities in those countries. It was pointed out that Facebook is now an identifier of first resort on e-bay to establish the reputation of the counterparty. The importance of trusted third parties for Internet transactions was emphasised. The requirement for individuals to retain control of their own identity attributes was also strongly supported.

Report from Workshop 2: Content creation in a changing world: How do we build the right environment?

The workshops that started many of the day's conversations were designed to produce substantive recommendations that lead to policy development and implementation. Of course, this is not quite so easy as it sounds.

Part of the problem, noted Alun Michael MP, was that many discussions of copyright are held between parties with shared interests in a separate room from those who disagree. However, when opposing parties are in the same room, discussions can turn contentious and delay action.

To forestall the usual back and forth on the issue, the chair of the workshop on content creation instead asked what we should expect on the issue ten years down the road. While one panellist declared that copyright would simply not exist in ten years, another pointed to the Digital Copyright Exchange proposed in the Hargreaves Review as a model that might carry copyright into the future, evolved to more appropriately fit the digital environment.

Several members of the audience spoke up to say they felt the question of copyright had to be at the core of any discussion around online content creation. There was general agreement in the audience, but they were more interested in talking about how we devise NEW models for copyright rather than how we enforce the old models.

The main points from the discussion were:

- We need to go back to basics and ask "what do we use the internet for"?
- What is content & who is producing it? It was agreed that 'content' is not just creative/storytelling, but information about anything.
- How do we take down the flags of nationality to create an equal and inclusive playing space?

- Instead of asking how do I get paid, ask who should get paid?
- Copyright model needs to change and move away from legislation to relationships & people
- With strong agreement from the audience, Alun Michael MP said we shouldn't ask the government to legislate as they would come down on one side or another – and the new & evolving Internet needs a more balanced approach to copyright. It needs to be more open & flexible.
- We need to look at legislation to promote platform impartiality for big content providers so as to foster an inclusive environment for independent platforms to develop, from the grass roots up.
- Arts & design - we need to find ways to connect the money with the creativity so (especially here in the UK where we have such a history of tech innovation) we can continue staying one step ahead of the curve with designing new technological & Internet solutions.
- We need to be building the future rather than just reacting to it

Report from Workshop 3: Cyber security: defining acceptable behaviour on the Internet

Mike StJohn Green (GCHQ, Former Deputy Director, Office of Cyber Security and Info rmation Assurance) outlined the framework for this workshop. The Internet now has over two billion users worldwide, with the greatest growth coming from developing countries. Cyberspace has been powerful in strengthening civil liberties, improving governments' responses to their citizens and promoting global commerce.

A commonly understood and accepted "standard of behaviour" could provide a framework for a trusted space. The aim of this session was to start the debate on identifying these standards.
Jamie Saunders (FCO) drew on the conclusions of the London International Cyber Conference of an Internet open to innovation and competition, open and without barriers to the free flow of information and ideas, where governments, industry and users work together, and where behaviour that is unacceptable offline is also unacceptable online whether it is carried out by individuals or governments.

How do we take this dialogue forward and to build a consensus? In particular we want to identify best practice: what could help promote the adoption of these approaches and build capacity? Do we need new initiatives?

Stephen Pattison (Director and CEO of the International Chamber of Commerce in the UK) noted that the reason we needed some sort of norms and principles was to give consumers and companies confidence in the Internet. The trick was not to fall into the trap of drawing up norms which were over prescriptive or which conceded ground on how the Internet is run. We needed Governments t be more focussed on these issues. There were a number of countries which wanted to see increased control over the Internet by governments, and would use this year's ITU Conference to further their objective. . It was important to show that a more cooperative, multi-stakeholder approach could be more effective. Business had to be more closely involved with Government's preparation for the WCIT Conference and for the Budapest Conference this year.

On the specific issue of cyber warfare and cyber crime, formal treaties might be relevant in cyber warfare, but otherwise needed to be approached with caution .

They were generally ineffective and often risked unintended consequences. A key to promoting cyber security was for Government to incentivise business to put better protections in place.

Simon McCalla (Technical Director, Nominet) agreed with the importance of a cooperative approach and noted that we had to think about where we are starting from: we are looking at this from our culture of multi-stakeholder engagement and of shared and common values. Some our ideas of acceptable behaviour might not be widely shared in a wider global context.

In the discussion, it was noted that many of the BRICS are facing the same challenges as us: they are interested in our approach. We need to show the economic benefits from an open Internet and understand the constraints that come from a state-centric approach, while addressing their concerns.

There was general agreement that the debate had failed to engage all the available expertise and gravitated to closed discussions. How can we use the resources that we have? This workshop aimed to reach a wider audience and improve engagement. However, there were concerns about the lack of communication, a barrier to wider engagement and outreach. There are risks, too. The identity-card debate led to more surveillance and data collection in society, and this might increase further with the exploitation of big data and the use of cloud computing. The definition of acceptable behaviour could lead to pressure for more controls on individuals.

In conclusion, the panel agreed that it was important to build around a consensus model on developing the Internet as a trusted space. Standards of behaviour mean different things to different countries and there is a risk of a push for a centrally managed approach to the Internet, with an impact on economic benefits. We agreed that the discussion needed to continue.