UK Internet Governance Forum

Report from UK-IGF event - 10 September 2013

What do we want from the IGF?

- Dr Vicki Nash, Oxford Internet Institute (Moderator)
- Mark Carvell, DCMS
- Lesley Cowley OBE, Nominet
- Andrew Puddephatt, Global Partners & Associates
- Kate Russell, freelance journalist

The moderator opened the session with a brief overview of the Internet Governance Forum (IGF) before handing over to Mark Carvell who outlined the learning experiences from IGF Baku. He explained that in their planning for this year the MAG were aiming for a much more interactive IGF. There will be shorter "flash" sessions and round table coordination for feeder workshops so the focus (main) sessions do not turn into a mechanism for simply reporting back from the workshops. Mark then moved on to discuss the UN's Commission on Science and Technology for Development Working Group (CSTD WG) on improvements to the IGF. At this stage, the group is not suggesting any substantial changes to the IGF mandate but welcome more tangible outputs, greater visibility, a more open and transparent process and broader participation – especially from developing and smaller states.

In response to a question from the moderator the panel outlined what they would like to see from the IGF going forward. Their suggestions were:

- Clearer leadership on matters critical to the health of the internet;
- Provide a monitoring function and an annual report/ assessment of state of internet;
- Develop evidence based policy options/ recommendations and shape the global research agenda;
- Improved website – this is the public facing front end but is unappealing and difficult to use. Better archiving and cataloguing of issues and topics on the website would mean it becomes a resource for policy makers. The website is missing the key messages, easily accessible headlines and highlights that would make the outputs dynamic and interactive;
- The IGF needs better marketing and publicity to make it approachable and consumable in order to broaden its reach and appeal. Without media interest the IGF is lacking wider appeal and sponsorship opportunities;
- The lack of Special Advisor is a major issue which has a serious effect on the profile of the IGF and causes it political credibility issues. In the current political climate, the IGF needs to communicate much more effectively to make the case for policy makers to be engaged in the process. Better recognition is needed from government stakeholders about the benefit of interaction with stakeholders in policy making;
- The establishment of the IGF was 8 years ago was groundbreaking. However, the environment was very different then. Greater thought needs to be given to the social, economic, technical and physical environment and how this will evolve and change going forward in order to ensure that the IGF is fit for purpose well into the future.

Dr Vicki Nash then invited audience comments and questions. The key points from the interactive discussion were:

- "Relevance" of the IGF is key – how it will relate to those who will participate now and in the future, especially in emerging markets.
- Further debate is needed on how concrete the decisions/ outputs should be.
- The multi-stakeholder model is the IGF's biggest asset - there needs to be more and better interaction between national and regional IGF's to build on this. The multi-stakeholder model was created to put pressure on govts. More action and engagement from industry is needed to avoid govt/ UN regulation. Governments should exert pressure on the UN.
- More emphasis should be on economic importance of the Internet and the effect of this on trust rather than focusing on the security issues.

- The IGF is impenetrable and needs to be more accessible to newcomers. The front line of these discussions should be on the internet with better facilities and more emphasis on remote participation.

There was strong feeling in the room that topics such as PRISM and wiki-leaks cannot be swept under the carpet. They have to be on the agenda to make discussions relevant. One audience member suggested that if this topic is not on the IGF agenda, that would be a fundamental failing and the IGF just becomes a mechanism for saying no to ITU control. There is a very real danger that politicians and the companies that know about it will not be able to speak about it – so the only noise on this will be from conspiracy theorists and people without meaningful knowledge on these topics. It was suggested that there is an opportunity for the UK to take a lead on this topic. It would provide an opportunity to address the transparency question on data law enforcement requests. We need to make sure we have something intelligent to say in order to ensure that it doesn't become a tin foil hat discussion. There is no reason to suspect that Snowden is the first person to access this information – he's just the first that has leaked. How do you balance between the offensive and defensive side of this – constructive dialogue and positive contribution? We need UK delegates to push for the elephant in the room discussion.

Parallel workshops x3

a) Identity & Trust (BCS, The Chartered Institute for IT)

Panel:
- Andy Smith, BCS (Moderator)
- John Bullard, Identrust
- William Heath, Mydex

This workshop was presented by the BCS and covered a number of areas related to the work of the BCS Identity Assurance Working Group. Andy introduced the workshop and the work the BCS is doing in this area.

William gave a short introduction on the incentives to go online. He opened with the hypothesis we are seeing the emergence of a new personal data ecosystem, one in which an individual's control of their personal data will play a significant and valuable role. This will have many benefits ranging from new business opportunities to better protecting human rights.

To do this we need incentives for three sets of actors; the individuals, the organisations that provide services over the Internet and the new breed of application developers such as those writing applications for iphone and android. Together they will form the ecosystems which will allow individuals to protect and manage their information.

At the moment the move to 'Digital by default' is being driven by cost reductions and providing better services. In order to do this the organisations need to be able to prove that people are entitled to the services they are asking for, through some sort of attribute verification. Coupled with this application developers want a predictable environment in which to create their applications.

One method of doing this is to use a trusted third party to provide identity provision, linking the individual to the organisations via new applications and tools while ensuring privacy and data protection under the control of the individual.

John then looked at trust and liability. He started with the question of "what is meant by Identity" He stated that it means "you have absolute certainty you know who you are dealing with" and you can check and validate that is the case and have someone that guarantees that the person asserting the identity really is the person they claim. There is also the need to have a clear resolution process in case things go wrong.

He explained how the parties interrelate and operate, making the point that in the global world of the Internet it is not possible to have a single organisation that would provide identity services or a guarantee of trust for everyone. Though you need a third party to provide that identity assurance and validate a persons identity, you need a method of doing this globally.

The finance industry has been doing this for many years. There is a trust model that works through the financial sector globally, as they have to do "know your customer" and for financial transactions to work they have to be sure of who all the parties are in a transaction.

He hypothesised that this capability could be used to provide the same capability for use of identity in any other transaction, with a trust model and liability model that is already in place today being expanded in scope to cover other areas where trust in an identity is required.

He emphasised that this would have to be done via the regulated financial industries as they already have the legal and regulatory models in place and can implement the necessary validation and liability models for use of identity in the future. This would include any regulated financial institution being able to validate an identity to any relying party via a regulated financial institution that the relying party trusts.

This does not need a global regulator, only that the regulated bodies trust each other, which they do today. This would require new rules and governance structures to take this model into the Internet era where you are not just talking about financial transaction but are also talking about other transactions with a liability model based on assured identity.

Andy then talked about the value of identity. Initially he covered the point that a person's identity attributes have value. Even though people think they are getting free 'stuff' on the Internet, they are actually paying for it by giving away identity attributes and information about themselves, which can then be used for targeted marketing, sold or data-mined for various purposes.

The information about who you are, what you buy, where you shop is all collected and used to support business on the Internet. However if the large organisations could not do this and did not have access to such information to drive their business models, they would have to find some other way of funding the services and software they provide on the internet. A simple example is software for the Android smart phones, where they is usually a free version which contains advertising and a paid for version which does not. Other examples are social media sites and search engines.

He stated that what we require is ensure that this stays in balance, that data protection and privacy do not become so onerous it disrupts funding of the Internet, but equally collection and data mining of personal information does not invade people's privacy or become uncontrolled. In the worst case such activity could become dangerous with people being targeted for nefarious activities.

He made clear that this is a balancing act and at the moment it is not in balance. If large organisations that provide popular services cannot collect and sell personal information or use it for targeted marketing those services would either become expensive or disappear. He then went on to show a number of forms that are used to collect information online, with examples showing that organisations are already collecting far more personal information than they need to offer their services and this is counter to the principles of a right to privacy.

He then made the point that filling in forms online with lots of personal information can be dangerous if you do not have a machine with good anti-virus software, as a keyboard logger on the machine could collect that information and send it to someone who could then steal or misuse your identity.

The final point covered was the issues around aggregation and data mining, with electronic databases being easy to search and cross-correlate it becomes much easier to build up a picture of someone's life or even find information about them such as their name and address from other attributes about them.

He then introduced the discussion section where questions were taken from the audience.

The first question was about what topics would be covered at UN-IGF. Andy explained that BCS is doing a workshop on the first day and the topics covered during this UK-IGF workshop, including input during the discussion, session would be fed in to that workshop.

Another question was that some of the statements made during the talks, such as the quote "if the product is free, you are the product" were a bit sweeping. The example given was that the BBC News website is free and that does not

collect personal information or do advertising. However the point was that the BBC News website is not actually free, it's paid for by the TV licence fee, which answered the question as to why there is no advertising on the website.

A point made was that collection of unnecessary information is already covered by data protection legislation and we do not need more laws, just better enforcement of the current ones. William made the point that we want an online economy based on an honest premise and people rights and protections should be fundamental to this.

The next question was around online jurisdictions and the models that had been discussed. If lawyers got together and agreed a model, how would this work. John pointed out this would it be based on the laws of contract with different layers providing a local perspective for the users or organisations but covered by a global contractual model similar to those currently used by Visa and Mastercard. The only contractual relationship the person would have would be with their identity provider.

There was a discussion on the UK Government GDS identity trust framework, which is a good concept and has gone a long way to solidifying the balance between provision of assured identity and provision of only those attributes needed for a transaction, reducing secondary use of personal information especially where the ability to do so is hidden in long complex online privacy statements.

The next contributor used to work for a newspaper and commented that when you signed up for an online subscription, all of that data was collected and sold off to marketing companies. This meant that each person's subscription data was worth about 12 pence. The question was is there a way that this value could be split between the organisation and the individuals? William who also worked in this area said he understood the model and it was possible to share the value, but this was not the individuals primary motivation, what they wanted was the subscription.

A company in the US tried this as a business model, but it did not work, as once individuals realised their data was valuable they wanted to retain the whole value. William also made the point that the value is not just about the personal information attributes, it's about a person's preferences, what they like, where they shop etc. This information has value for targeted marketing.

There was then a discussion on supermarket loyalty cards and the pros and cons of these. At least with such loyalty cards people know who they are sharing the information with and for the most part what it is being used for. They expect targeted marketing from the supermarket.

There was a short conversation on the use of new application types such as heart rate monitors which can record a person's heart rate over extended periods and store this information online. This information is also being sold off, supposedly as anonymised data but in some instances personal attributes have been included with the data sets which allow though data mining the individual to be identified. These are the sorts of accidental secondary uses that need to be better controlled.

Andy then introduced one of the topics that will be covered at UN-IGF, which is the balance between security, privacy and anonymity. This solicited a useful discussion on the topic and as usual provided strong opinions on both sides of the argument.

The point was made that security and privacy are actually mutually supporting and are both good things. It is anonymity and its ability to support nefarious activities that is the bad thing. Andy pointed out that the underlying problem is that there is too much personal information on the Internet and once something is published it is virtually impossible to redact or remove it. This means the Internet is a huge data warehouse that can be mined. He stated that we need to improve privacy online, but that does not mean we need to make things anonymous.

The discussion went on to identify that anonymity and privacy are very contextual and depend on the transaction and context in each case. The view was that this whole area is far more fragile and nuanced than the discussions currently address. Much more debate is needed that should move away from what is good and bad and look with a more nuanced view of the context around the use of anonymity and privacy and how they interrelate. There was agreement that there are very strong opinions both ways and this will not change any time soon.

A comment was made that attribution is something that needs to be taken into account here. Anonymity and attribution are interrelated and can be used to improve the balance. Being able to attribute an action to a person may be necessary in one context such as solving a crime, but this may not be needed in general use in which case the attribution could be anonymous.

William pointed out that a good challenge had been set by one of the audience to be taken to UN-IGF, and that a simple proposition should be put forward that users should have more control of their personal data and governance of the Internet should address this specific issue. This does not stop business exploiting personal information, but it would be more under control of the individual.

Andy made a comment about the scale of the Internet and the fact information is virtually never deleted. This makes aggregation and data mining all the more effective and dangerous. He asked the audience for their views on the ability to withdraw consent. Everyone agreed that this was a good idea, but the practical aspects around this would be very difficult to implement.

Williams point was we now have a totally organisational centric structure on the Internet which has been built up over many years. We need to start thinking about user centric data models. We need to move to a more balanced view with individual centric aspects being seen as just as important as organisational aspects. There is the ability to get copies of all the information held about you, but there is currently no way to enforce the removal or redaction of personal information online. Another point was that given all the copies, caching and archiving it would be very difficult to implement data removal.

There are also other aspects that need to be considered such as legislation covering know your customer and record retention which may prevent removal. However postings on social networks and news groups should not retain information that has been deleted by the individual.

The discussion moved on to the ability of online organisations such as social networks to change their privacy policy without the users consent. Andy answered this and made the point that one social network he had been a member of kept changing the privacy policy and the last change meant that they owned all your photos, at which point he removed his account which was the only choice other than agreeing to the policy.

However most people will not have read the policy and will not realise that all of their pictures are now owned by the social network. Most teenagers may not care about this today, but may in the future when such pictures impact their livelihood or ability to get a job. There is a whole area that needs to be address about protecting the naïve from themselves.

William made the point that there is a dichotomy for some organisations as they are stewards of personal data on the one hand, but have an obligation to maximise profits for shareholders on the other which can lead to a conflict of interests. This means in some instances they cannot be regarded as responsible stewards of personal data. Even if they have the best intentions they may in the future be forced to sell the personal information as an asset of the organisation.

The last point made was privacy can be thought of as security by obscurity as for the most part it prevents access to the information, however where it is required such as for law enforcement it can be obtained and most legislation such as the Data Protection Act does have clauses to allow for this. This also means that anonymity online is extremely difficult to achieve as everything from the end IP address onward is recorded somewhere and can be obtained with the relevant authority.

At that point the discussions were closed.

b) Internet governance principles in a changing international environment (Global Partners)

Panel:
- Matthew McDermott, Access Partnership (Moderator)
- Kevin Brind, FCO
- Marianne Franklin, Goldsmiths/Internet Rights and Principles Coalition (IGF) - remote panellist

- Nigel Hickson, ICANN
- Malcolm Hutty, LINX
- Matthew Shears, CDT

This panel session looked at the role of Internet governance principles in maintaining the multistakeholder model. With the global IGF and other international fora all looking at what some are calling "constitutional" issues surrounding the Internet, existing and proposed principles are under heavy scrutiny, as stakeholders search for a set of common rules by which everyone agrees the Internet should be governed. The panel, including representatives from the business community, civil society, and government, familiarised the audience with notable national and international initiatives, and discussed with the audience how the UK can most beneficially advance the debate.

WHY DO WE HAVE INTERNET GOVERNANCE PRINCIPLES?Panellists suggested a number of different reasons for why we should have Internet governance principles, including supporting UK business, and ensuring human rights on the Internet are not taken for granted. It was agreed that that there is a tension between the needs of business and civil society, and that principles need to strike a balance between the two.

It was also argued that principles, while not having the force of law, help to bind us together, and provide a context within which the Internet governance debate can happen. However, some noted with concern that principles tend only to be followed by countries and organisations that had a hand in drafting them.

HOW DO WE PICK BETWEEN PRINCIPLES? At the IGF there will be an analysis of 28 different sets of principles from around the world to determine where there are elements of commonality. While this was seen as an important activity, some panellists were concerned about how a set of principles is selected for the list, and whether certain stakeholders will be excluded from the process.

It was suggested that the starting point for any selection of principles should be international law. Companies conduct business every day based on the understanding that international law will prevail, and principles should not be written in a way to jeopardise those rights.

DO WE NEED UNIVERSAL PRINCIPLES? It was suggested during the debate that there is a global demand for universal Internet governance principles. Rather than continuing to support a proliferation of principles from different organisations and countries, we should focus our attention on a single set of principles that can be adopted by all; we need to quickly identify core areas of agreement and use the multistakeholder model to get them adopted. It was suggested that unless supporters of the multistakeholder model take the lead on this action the UN will do it for us.

Others suggested that we need to focus on domestic issues and that principles will necessarily be solutions to national concerns. However, there was agreement that the development of principles has a role in maintaining a single Internet, and buttressing support for the multistakeholder model.

ADVANCING THE DEBATE - While there was uncertainty over what the IGF could achieve in examining different sets of principles, it was agreed that it was a useful initiative and that the results could provide direction to the debate. It was also agreed that the UN has a role in helping both the development of principles, and also their adoption. However, there was no clarity on how the UN would fit into the existing processes for creating Internet governance principles.

There was a concern that the proliferation of principles could cause problems, leading to a devaluing of the concept. However, it was felt that this concern is outweighed by the importance of developing common points of reference, and that all stakeholders should continue to work with as wide a range of actors as possible, and avoid the development of a balkanised Internet.

c) **UK priorities for the Seoul Conference on Cyberspace (Foreign & Commonwealth Office) - Harpley Suite**

Panel:
- Jamie Saunders, FCO (Moderator)
- Dr Ian Brown, Oxford Internet Institute
- Gabrielle Guillemin, Article 19
- Konstantinos Komaitis, ISOC

- David Pollington, Microsoft

The purpose of this panel was to provide an update on planning for the Seoul Conference on Cyberspace, scheduled to take place on 17th-18th October, and to seek views from UK-IGF members on what specific outcomes and deliverables we should be seeking to reinforce. The panel was drawn from Government, Industry, Civil Society and Academia.

The broad scope of the Seoul conference was described - this covered the role of cyberspace in promoting economic growth and social progress. Security was also an important theme, but as an enabler of growth and progress, not as an end in itself.

The anticipated outcomes of the conference fell into three broad categories:

- Policies. Using the conference as a platform to promote progressive policies for countries to adopt at the national level and for us to champion at the international level - eg promoting the open nature of the Internet, the multi-stakeholder model, and human rights. It was not enough to point to high level principles - we needed to point countries towards practical policy models that could be implemented in their local contexts.

- Capacity Building. Our narrative on the benefits of cyberspace risked being undermined by a failure to close the digital divide and help countries to create the conditions for real growth in their digital economy. Critically, this included helping countries to develop approaches to cybersecurity that would help them prevent their investments in infrastructure being undermined by a failure of end user confidence and trust.

- Cooperation. There were significant obstacles in the way of effective international cooperation to enable countries to work together to maintain the security and resilience of cyberspace. The conference needed to put forward practical measures to address this gap.

Various suggestions came up during the course of discussion and during the Q&A. The importance of supporting the creation of local content was seen as critical - use of open standards would help keep costs of entry for local players down. The importance of promoting progressive policies on freedom of expression and privacy protection was highlighted by many - it was important to ensure that calls for necessary security were not subverted into calls for censorship and control. We needed to ground our efforts in the practical - there were a number of good policy models out there - how could they best be implemented? Genuine multi-stakeholder engagement was seen as a valuable way of keeping policy grounded and for holding Governments to account - some Governments and institutions were better at this than others. All agreed on the importance of focusing on emerging economies and of the need to understand needs for their perspectives - Seoul was a valuable opportunity to promote progressive policies, but needed to be made relevant to countries struggling to do the basics.

The proximity of the Seoul Conference to the Bali IGF was noted. The involvement of Foreign Ministers and other "non-specialists" at Seoul was a good opportunity to raise issues that might not otherwise attract attention from those outside the IGF community.

Infrastructure issues – IPV6 & Spam

Panel:
- Olivier Crepin-Leblond, ISOC England
- Mark Carvell, DCMS

The IPv6 Matrix project checks for IPv6 connectivity of the 1 million most popular Web sites worldwide. A fair number of them are based in the UK. However, the UK server pool is poorly connected to IPv6: whilst the figure for Germany is 6.99% and the European Leader Slovakia at 13.94%, only 0.5% of sites are connected via a dual stack IPv4 and IPv6 %.

One of the reasons for this poor record is the lack of pro-activity from the government to actively mandate IPv6 in its IT procurement contracts. It was also found that a false sense of comfort with the availability of IPv4 addresses in the UK made it unattractive to invest in updating networks to run IPv6. Unfortunately, the 6UK initiative failed to change this perception. With no demand, there was no incentive for supply.

A call was made for all those present, to promote the use of IPv6 in their organisation. Without a widespread roll-out of IPv6, the UK software developer community would be disadvantaged compared to its European neighbours.