UK-IGF Planning Meeting – 15th May 2017

Time: Mon 15th May 2017, 17:00 - 20:00
Host: BCS, 5 Southampton Street, London, WC2E 7HA

Topic 1 – Mental health online & accessibility

Rachel O'Connell

Social Media gathers a lot of information about people and this can be triaged to help identify those vulnerable and to target appropriate support services to them. Several issues arise from this:

- Data protection/Privacy
- How to get the relevant information to the correct people
- What is the duty of care of Social Media platform?
- How to make sure services are accessible to all (including the vulnerable)
- What should oversight/governance frameworks look like? At present, there are none.

Good practice exists: E.g. Big White Wall, which has had a lot of success with US war veterans.

eID solutions can be part of the answer in ensuring users can only access age appropriate services.

Comments from the floor

The Design Museum is showcasing some innovative apps designed to address health issues such as:

- Self-harming
- Dementia

Accessibility for the less able is a big concern in general and especially in this area if services are to reach those most in need of them.

If a new technology was generating as much harm to the physical health of users as some argue social media is to mental health, especially that of the young, there would be an immediate call to action. This should not be overlooked.

Some sort of research/analysis to generate some quantitative assessment of the scale of the problem would be useful and would help any call to action gain traction.

There could be some cross-over into the area of govt monitoring or surveillance, which some argue are having effects on peoples' mental health. Consequently, it'll be necessary to define the scope of any discussion carefully to avoid this.

It should be remembered that tech will be part of the solution and not just the cause of the problem. A balanced view to reflect this will be important.

Key issues/Possible outputs:

- Good governance/Best practice codes for social media

- Agreed standards for tech solutions
- What policy innovations are needed to enable tech solutions

Topic 2 – World Bank Group principles on Internet Governance

Introduction from Louise Bennett

The WBG principles were published in 2017 and it's surprising that the UN-IGF was not involved in their drafting and has not formally endorsed them. The principles seem well crafted and cover three areas:

- Inclusion/Access
- Design/Resilience
- Governance/Trust

A strength of the principles is that they are not perceived to have come from Europe or the US, which has been a barrier to wider acceptance in the past.

John Bullard & Andrew White

- The principles support the WBG desire for sustainable development
- They are succinct & clear
- A key component is an online identification scheme
- Keeping the principles simple was an admirable and ambitious goal, but the consequence seems to be that some necessary elements have been neglected such as any discussion of liability

Concerns regarding this topic are that the area is very complex and it may be that the regulatory framework is not yet mature enough to allow any meaningful progress to be made.

Comments from the floor

It was argued that there is some discussion of liability/accountability within the principles and their simplicity may encourage adoption, which would improve things even if only by a small step.

The UK has its own embryonic ID scheme called Gov.uk Verify and if this could be aligned with the WBG principles, then it might give an international element to the UK's work.

Perhaps the UN-IGF should be lobbied to adopt these principles. In general, the internet does need a universal ID solution if it is to work properly.

The Open Banking Community has found it difficult to persuade 3rd parties to adopt appropriate eID standards so that they can ensure secure transactions. Pressure on UK Treasury would be welcome.

In general it seems that this could shape up into an important discussion, but it is quite a technical subject. Perhaps a speaker from the Cabinet Office would be a good idea.

Topic 3 – Fake News

Olivier Crépin-Leblond

This is not a new phenomenon, but it is a hot topic now. The phenomenon appears to be magnified by the internet and it now seems to effect elections and effect stock market prices. So, some key concerns.

Today the pressure to be first to publish seems to override the desire to check and verify facts. But how is fake news defined and detected? How do the algorithms that platform providers use in an attempt to solve this issue work?

Comments from the floor

This is clearly a fascinating topic, but one concern would be how to make it output orientated. What could the output be? Will it still be a hot topic in September?

As a counter to this it was suggested that there are ways to frame the issue to address interesting questions. It may be worth considering whether the term 'fake news' is by definition a construct of users of conventional news media and is a concept that younger consumers of media don't recognise. Perhaps the term 'fake news' should be avoided and instead discussion focussed on issues such as:

- What liability/responsibility do platform providers have?
- What analytics are used to target certain content at certain users?
- Should there be greater transparency about what information is served to whom?
- What is the role of commercial drivers in targeting certain information to certain users?
- Should there be additional safeguards with respect to political messaging?
- Is there a principle at stake here? Specifically, our right not to have our views manipulated.

This topic, and particularly the last point above, could feed into a wider discussion about how respect for human rights can be built into internet governance.

Topic 4 – Cyber security & Privacy and Topic 5 – IoT

Carsten Maple & Bill McCluggage

Clearly this topic must be included in the programme. Given recent events it would be an odd decision to exclude it. The key issue will be to get under the hood of it and work out what the angle should be.

There is a lot of discussion about GDPR and its interfaces with IoT. Some key outputs could be:

- Principles or guidelines about how to manage consent, especially in environments where the landscape of what you are consenting to can change.
- How can active consent work? How can it be implemented for people of all ages?
- What liability framework should there be for complex systems were separate parts have different data processing roles?
- What are the effects of machine learning?
- How can verified parental consent for access to children's data be managed?
- How can age verification models work? What is the value of de-coupling age from identity?

Comments from the floor

At present, it seems that methods of attack are cheap and defence measures are expensive. From an engineering perspective, the internet has been poorly designed and does not effectively separate data from function. A key question is can the fundamental architecture of systems be modified to redress that imbalance? There needs to be more advocacy for the concept of privacy by design.

In general, the additional complexities that IoT bring make the overall picture scary. Some cyber security best practice guidelines for businesses and individuals could be another key output.

Topic 6 – Education – Moral & Ethical

Jeff Day & Rachel O'Connell

The online world presents challenges for the young. In today's world our children can be exposed to a wide range of materials and experiences before they've had any advice on how to deal with them. Parents often feel powerless and unable to help their children.

The consequences of not dealing with these issues can be child exploitation and radicalisation, so the imperative for action is strong.

Comments from the floor

Examples of best practice in this area:

- CyberCenturion in the UK
- CyberPatriot in the US
- The Estonian Govt has a good initiative

The Institute for Statecraft is working on a cyber security education programme for 10 – 16 yr. olds.

Again, it's worth noting that in addition to user education there can be technical solutions such as systems to allow users to verify their age and only share their content with those of a similar age.

A key focus could be how to develop programmes to:

- Help the young understand and deal with the online world.
- Teach critical thinking and ethical decision making

It was agreed that the youth panel session was very valuable at last year's event. At the very least this should be repeated and it would be good if youth involvement could be expanded to learn their perspectives across all the subject areas.

General Comments

There was strong support for the inclusion of topics 1 & 4, but all topics were considered of value. The ambition of the group was that the eventual programme should cover all the areas if possible.

To achieve this while keeping the audience engaged, thought should be given to varying session formats and considering the use of break-out sessions.

A key objective should be to generate outputs that can feed into UN-IGF discussion sessions or best practice working groups. There may be some good fits for the 2017 UN-IGF, while other UK IGF topics may need to be targeted for 2018.

Remembering the overall theme for UK IGF 2017 is 'Shape Your Digital Future!' one suggestion for an overarching strand is to promote the mainstreaming of human rights within Internet governance. Arguably, this is compatible with many of the topics set to be discussed.