UK Internet Governance Forum

UK-IGF 2017 – Looking ahead to Geneva

Cyber-Security: Building a Policy Response to an Eminent Threat

We are facing a significant, ever more complex, and fast-moving threat landscape. Priorities include:

- Greater boardroom awareness of cyber threats and risk analysis.
- Measures to fill the skills gap for cyber professionals.
- User education, savvy and empowered users will be key.
- Fit for purpose regulation that sets internationally agreed standards.

Governments must engage across all relevant departments. Equally, however, governments can't provide solutions alone, academia, industry, and the individual all have parts to play.

Cyber Resilient Businesses

In order to build their cyber-resilience, businesses need to:

- Improve their understanding of their exposure to risk.
- Employ a holistic approach. It's not just about secure kit, it's about secure processes.
- Be prepared to invest in appropriate resource.
- Be open to independent review of their capabilities.
- Record and track cyber incidents in order to better learn the lessons.

Education and Online Safety: Informed Digital Citizens

The key to resilient children is a balanced view of the impacts of tech and solutions that move beyond just restricting and blocking. Young peoples' right to online access must respected, but balanced with their right to a safe environment. Policy frameworks should seek to:

- Empower the young to speak-out, so we can better understand their views and experiences.
- Use young people as educators of both their peers and of relevant professionals.
- Provide mechanisms to build community resilience by allowing young people to share their experiences and look-out for each other.

Mental Health and Accessibility Online

Platform providers must accept responsibility and move beyond solutions that push the onus to act back onto members of the online communities in question. The time to act is now, and we should take a positive view of the roll that technology can play. It should be noted that:

- Technical solutions exist that can help to identify those most at risk, so they can be targeted for appropriate interventions.
- The right systems can allow mental health professionals to buy into this type of approach.
- The identity as a service industry is coming, meaning it should be possible for platforms to mitigate risk by ensuring that the content they serve to users is age appropriate.

- Timely interventions can head-off greater problems in the future, offering both better outcomes and cost savings.

Fake News

The very term 'fake news' may be part of the problem as it conflates two very different issues, frivolous stories designed to harvest clicks for revenue and the much more harmful state sponsored dissemination of misinformation. They are two distinct phenomena, with distinct motivations, and they mandate different policy solutions.

- Social media providers are doing more to fact check and to empower users by branding content from known sources. They are reluctant, however, to be the arbiters of the truth.
- An over-playing of the scale and impact of the problem could lead to poorly crafted regulation.
- The phenomenon reflects wider societal issues and we should not expect the social media providers to solve the problem for us.
- That said, many believe that platform providers must take more editorial responsibility.
- It's clear that there is unlikely to be a technical solution.
- Steps to improve digital literacy will be key. It's widely agreed that we all need to be better equipped to assess the provenance of what we read online.

Shaping your Digital Future – World Bank Principles on Identification

The principles covering inclusion, universal coverage and accessibility seem broadly sensible and could usefully apply to many aspects of the digital world, not just ID systems. But:

- Systems must be accessible by means or at locations relevant to vulnerable groups.
- Achieving this is likely to require co-operation between governments and the education, business, and health care sectors.

A system design based on open standards, will enable a degree of trust by scrutiny. That said, creating a robust, secure, responsive, and sustainable ID system presents significant challenges:

- A system required to operate for a full human lifespan must be sufficiently future-proofed.
- Scope creep beyond ID should be avoided as collecting more data will undermine user trust.
- Funding is a challenge. Any commercial angle could threaten the purity of the concept.

Turning to governance and protecting privacy and user rights, challenges include:

- How to accommodate differing legal frameworks with respect data use and disclosure.
- Establishing enforcement processes that can work across borders. If a single over-arching legal framework is required, how can that be agreed?

None-the-less the principles represent a useful contribution and further endorsements should be encouraged. The UN-IGF is currently working to develop a similar set of principles and a useful start would be for the UN-IGF to co-opt the ID4D principles thus avoiding a duplication of effort.

Human Rights

One overarching principle that should not be forgotten is that the sorts of frameworks and principles that protect human rights offline, should also apply online.