UK Internet Governance Forum

Report from the UK-IGF 2017

REPORT FROM THE UK-IGF 2017

The UK Internet Governance Forum (UK-IGF) is a collaborative partnership between Nominet, the UK Department for Digital, Culture, Media & Sport, key parliamentarians and other organisations taking a leading role in making the internet a better place. The event aims to provide a UK forum 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.

The 2017 UK-IGF was held on 13 September in central London and gave delegates representing a broad spectrum of stakeholder perspectives the opportunity to join wide ranging discussions. Views were heard from The Rt Hon Matt Hancock, the UK's Minister of State for Digital, other parliamentarians, as well as from experts representing key government agencies, the internet industry, academia, and wider civil society.

This report outlines the core themes that emerged from a day of lively discussion and debate.

CYBER-SECURITY: BUILDING A POLICY RESPONSE TO AN EMINENT THREAT

Panellists

Gordon Morrison, McAffee UK (Director of Government Relations)
Richard Holmes, CGI Cyber-Secure Systems (Secure Systems Engineering Director)
Dr Bob Nowill, Cyber-Security Challenge UK (Chairman)
Prof. Christopher Hankin, Imperial College London (Director of the Institute for Security Science and Technology)
Senior Speaker, National Cyber Security Centre

This session examined the growing cyber threat to the UK's critical national infrastructure and to consumers through their connected devices. Discussions explored what the role of governance should be and what a policy based response might look like.

There was broad agreement that the threat is significant and growing. IoT applications mean the number of connected devices is set to grow exponentially and developments in AI will only add to an ever more complex and fast moving threat landscape.

Priorities identified if the vision of a prosperous and confident digital UK is to be met are:

- Greater boardroom awareness of cyber threats and risk analysis.
- Measures to fill the skills gap for cyber professionals.
- Improved user education, savvy and empowered users will be key.
- Fit for purpose regulation that sets internationally agreed standards and focuses on broad principles, not operational details.

Delegates agreed that given the scope of the response required, government must engage across all relevant departments. Equally, however, government can't provide solutions alone, academia, industry, and the individual all have parts to play.

CYBER RESILIENT BUSINESSES

Richard Horne, PwC (Cyber-Security Lead)

Delegates heard how businesses can 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.

Greater cyber resilience in the business world will depend on the active participation of all of us engaged online and a considered approach from policy makers.

MINISTERIAL ADDRESS

The Rt Hon Matt Hancock MP, Minister for Digital at the Department for Digital, Culture, Media and Sport

Delegates heard a wide-ranging speech from the Rt Hon Matt Hancock MP, the UK's Minister for Digital, in which he called for the UK to play a leading part in the Internet governance debate drawing on a degree of self-confidence in our shared values.

You can read the full text of the minister's address here

EDUCATION AND ONLINE SAFETY: INFORMED DIGITAL CITIZENS

Panellists

Hannah Broadbent, Childnet (Deputy CEO)
Sophie Linington, Parent Zone (Deputy CEO)

This session focused on how society can encourage the young to become informed and responsible digital citizens and considered what role policy can play in shaping and encouraging best practice.

Delegates heard that the key to resilient children is a balanced view of the impacts of tech and an environment that supports young people's choices and doesn't just react by restricting and blocking. Children who fear loss of access to their devices frequently opt not to report abuse. Young peoples' voices must be heard and their right to online access respected. That right, however, must be balanced with their right to a safe environment. Our policy framework should seek to:

- Empower the young to speak-out, so we can better understand their views and experiences.
- Tap into the potential of young people as educators of both their peers and of professionals in the education and social care sectors.
- 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

Dr Rachel O'Connell, The Trust Bridge (Founder and CEO)

Delegates heard some compelling messages on the impacts the internet and social media can have on the mental health of users.

It was noted that the industry has tended to push responsibility for ensuring user well-being back onto members of the online communities in question. This approach should change and technical solutions do exist that can help to identify those most at risk, so they can be targeted for appropriate interventions by qualified professionals. Despite some initial reluctance, 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. It should also mean that younger users can be sure that the content they are sharing online is seen only by their peers.

The session ended with a call to action for industry players, noting that timely interventions can head-off greater problems in the future. This seems particularly important at a time when the resource available to mental health professionals in general is being squeezed.

FAKE NEWS

Panellists

Mark Wood, Nominet (Chair)
Carl Miller, Demos (Research Director)
James Cook, Business Insider UK (Tech Editor)
Chi Onwurah MP, Shadow Minister for Industrial Strategy
Simon Milner, Facebook (Policy Director for UK, Middle East and Africa)

A lively debate discussed the topical issue of fake news, what editorial responsibilities should be incumbent on social media companies, and the role of commercial drivers and algorithms in targeting certain content to certain users.

Discussion quickly revealed that one problem is defining what exactly is fake news. Frivolous stories designed to harvest clicks for revenue are frequently conflated with the much more harmful state sponsored dissemination of misinformation. They represent two distinct phenomena, with distinct motivations, and consequently mandate different policy solutions.

Delegates heard that social media providers do care about the quality of information on their platforms and are doing more than ever to fact check where appropriate and to empower users by branding content from known sources. They are reluctant, however, to be the arbiters of the truth and are concerned that an over-playing of the scale and impact of the problem could lead to poorly crafted regulation. This view was echoed in comments casting fake news as a wider societal issue and cautioning that we should not expect the social media giants to solve the problem for us.

Discussion noted that while there is regulation governing political messaging offline, there is no such regulation online. Some expressed the view that this represents a regulation deficit that should be addressed, while others cautioned against over-regulation that could prove anti-competitive, or worse, could offer a back-door route to state surveillance. Overall, however, there was strong support for the view that platform providers must take more editorial responsibility.

There were calls for greater transparency over how algorithms target certain content to certain users. How such transparency can be meaningfully delivered, however, was questioned. Most users will not read through a long list of Ts & Cs. Nor will they have the skills to decipher pages of code.

The debate closed with no firm consensus on many aspects of the issue. There was, however, clear agreement that there is unlikely to be a technical solution. Instead steps to improve digital literacy will be key. 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

Breakout sessions chaired by:

Inclusion and Access – **Natalie Campbell,** Nominet Trust (Chair)
Design and Resilience – **Adam Peake,** ICANN (Senior Manager, Accountability)
Governance and Trust – **Louise Bennett**, BCS Security Community of Expertise (Chair)

The final session of the day gave delegates the opportunity to explore the theme of individual online identity. Inclusive, secure, and trustworthy identification systems are key to ensuring individuals can participate fully, socially, politically, and economically in the digital age.

In 2016, however, the World Bank estimated that 1.5 billion people in developing countries have no means of proving who they are and argued that this identification gap represents a significant barrier to global sustainable development.

The Identification for Development (ID4D) initiative has responded to this challenge by setting out 10 principles that they believe should underpin digital identification systems. Delegates examined these principles, considering whether they are fit for purpose and whether there should be a push for the UN-IGF or UK Government to join those endorsing them.

The first set of principles covering inclusion, universal coverage and accessibility were broadly supported by delegates who felt they could usefully apply to many aspects of the digital world, not just ID systems. One challenge identified, will be to ensure systems are accessible by means or at locations relevant to vulnerable groups. Achieving this is likely to require a broad conversation between governments and the education, business, and health care sectors.

Turning to design, delegates felt there were significant challenges in ensuring a robust, secure, responsive, and sustainable system. How can a system required to operate for a full human lifespan be sufficiently future-proofed given the pace of technological innovation? There were also concerns over whether there might be a temptation for scope creep beyond just ID in a way requiring more data-sets to be captured and, therefore, likely to undermine user trust.

There was clear support for the use of open standards, enabling a degree of trust by scrutiny. Further concerns focussed on financial sustainability, what will be the funding model? How can funding be secured in a way that does not require a commercial angle that could threaten the purity of the concept?

Finally, turning to issues of governance and how to build trust by protecting privacy and user rights, delegates considered the challenge of differing legal frameworks with respect to data use and disclosure and how any enforcement processes could work across borders. The concepts of enforcement audits and an ombudsman were suggested. Ultimately, however, delegates felt that a single over-arching legal framework would be required and securing agreement on what that should be could be difficult.

In closing this session, delegates noted that despite their reservations 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.

You can keep up to date with the work of the UK-IGF by visiting our website at

www.ukigf.org.uk