UK INTERNET GOVERNANCE FORUM REPORT - MESSAGES FROM LONDON

22nd November 2018

Cavendish Conference Centre,

22 Duchess Mews, Marylebone,

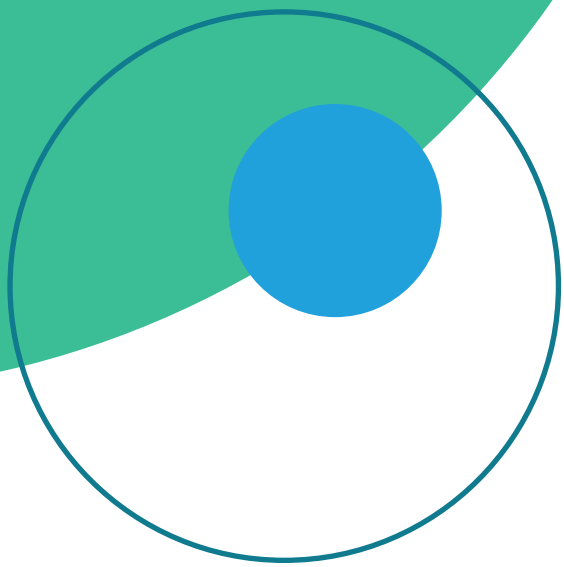
London W1G 9DT

UK IGF 2018

The UK Internet Governance Forum (UK IGF) is the national IGF for the United Kingdom. IGFs are an initiative led by the United Nations for the discussion of public policy issues relating to the internet. A key distinguishing feature of IGFs is that they are based on the multi-stakeholder model – all sectors of society meet as equals to exchange ideas and discuss best practices. The purpose of IGFs is to facilitate a common understanding of how to maximise the opportunities of the internet whilst mitigating the risks and challenges that the internet presents.

The UK IGF has a steering committee and secretariat. The committee members can be found here and the secretariat is provided by Nominet, the UK's national domain name registry. If you are interested in contributing to the UK IGF, please contact info@ukigf.org.uk.

The 2018 UK IGF was held on 22nd November in central London and gave delegates representing a broad spectrum of stakeholder perspectives the opportunity to join wide ranging discussions. Views were heard from Margot James MP - Minister for Digital and the Creative Industries, 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.



NOMINET Access Partnership Department for Digital, Culture, Media & Sport GLOBAL PARTNERS DIGITAL Internet Society UK England Chapter linx

OPENING REMARKS:
Russell Haworth, CEO, Nominet

Russell Haworth, opened the UK IGF 2018 noting Nominet's proud support for the 10th year. He thanked the Minister for her leadership to help make the UK one of the safest places to be online. Through running the .UK infrastructure and providing cyber security services to the government, Nominet is alive to the ever-present challenge of keeping the digital world safe and secure. He noted the importance of the topics discussed today, including the prevention of online harm, the improvement of security, protection of data and implications of emerging technology. He reminded attendees that the UK IGF is one of many multi-stakeholder conversations on internet governance and decisions from a range of international organisations, such as the Internet Engineering Task Force continue to have wide ranging implications for society, security and the digital economy.

KEYNOTE SPEECH:
Margot James MP, Minister for Digital and the Creative Industries

Margot James MP, the Minister for Digital and the Creative Industries, set out some of the key priorities for her department. She highlighted the need to work closely with all stakeholders - from business, civil society, representatives of users, and from the technical community - so that our policy decisions are shaped by practical concerns, not abstract theory. The proposals in the forthcoming white paper will need to include: protecting freedom of expression; promoting growth, for example by protecting SMEs; and supporting people's ability to adapt to technological change. She explained that the Digital Charter is the flagship DCMS strategy on digital policy, including internet safety. The proposals in the forthcoming white paper will need to include: protecting freedom of expression; promoting growth, for example by protecting SMEs; and supporting people's ability to adapt to technological change. The minister also described the importance of maintaining the ability to exchange data with the EU after Brexit. She highlighted that 75% of cross border data flows are within EU and noted that the adequacy assessment process will start at the beginning of the transition period and will be a priority.

AI EXPLAINER:
The potential impact of AI on my generation, and how we can plan for the future

Kari Lawler, Founder of Youth4AI, explained her journey to become one of the UK's youngest ever start-up entrepreneurs and one of the top ten teen female tech talents in the UK. Youth4AI aims to help 13-25 year olds learn about AI. She explained that the concept of Artificial Intelligence (AI) is often misunderstood. The mainstream media tends to overstate what is currently possible and portray the future of AI in a negative and dystopian manner. She explained that this has created unnecessary fear among younger people - Generation Z. She encouraged education to help Generation Z proactively plan their future careers in the context of AI developments. She also challenged society to consider whether the current level of data collected about individuals was desirable, and if not - contemplate how we could improve this.

ONLINE SAFETY:
Making the UK the safest place to be online

This goldfish bowl panel discussed how the UK can become the safest place to be online with a focus on cyberbullying, hate speech and marginalisation.

Panellists

- Professor Sonia Livingstone, Professor of Social Psychology, London School of Economics
- Douglas White, Head of Advocacy, Carnegie Trust
- David Wright, Director, UK Safer Internet Centre
- Vicki Shotbolt, Founder and CEO, ParentZone
- Barbora Bukovska, Senior Director of Law and Policy, London Article 19
- Andrew Honeyman, Head of Online Harms White Paper and Regulation, DCMS
- Jodie Ginsberg, Chief Executive, Index on Censorship

The panel considered various frameworks to define online speech, noting the need for clarity over what is acceptable online. Some panellists were concerned that the term 'hate speech' was being applied too widely in order to close down legitimate freedom of expression. They noted the need to differentiate between problematic speech that is illegal and problematic speech that is not illegal but could be offensive or harmful.

International law was raised as a framework for understanding problematic speech. The most severe forms of problematic speech (incitement to genocide, violence, discrimination and hostility) are expected to be criminally restricted. Other speech can be restricted in certain contexts, for example in schools or work places. A final larger category of speech can be problematic for social cohesion but is generally not restricted under legislation. It was suggested that policy solutions for this category of speech should focus on improving education, increasing social mobility and reducing poverty.

The panel considered whether existing UK regulation was sufficient for application to digital platforms. Some panellists recommended that additional training and resources were needed to support police understanding and enforcement of existing laws. There was general agreement that greater public oversight of decisions to restrict content could improve transparency and accountability. Panel members proposed different solutions for creating this oversight. This included a duty of care model – where social media platforms have a duty of care towards their users, and an outcome-based model – where companies are allowed to create unique technological and process solutions to achieve the specified public interest outcome. The panel noted that technical solutions may not always be appropriate and the challenge of large volumes of potentially problematic content.

One panellist recounted seeing parents becoming increasingly risk averse and even becoming fearful of searching for guidance and information on inappropriate content. The panel emphasised the benefits of online engagement and a desire to ensure children and young people could participate in the positive connections and learning offered in a digital age.

Andrew Honeyman, Head of Online Harms White Paper and Regulation, DCMS provided an overview of the UK government's current work on online harm. Following the publication of the Internet Safety Strategy Green Paper in October 2017, DCMS ran a consultation period that concluded in December 2017 and the government published its response in May 2018.

The consultation covered various aspects of online safety including:

- The introduction of a social media code of practice, transparency reporting and a social media levy
- Technological solutions to online harms
- Developing children's digital literacy
- Support for parents and carers
- Adults' experience of online abuse
- Young people's use of online dating websites/ applications

The consultation found there was strong support across all sectors, including technology companies and charities, for the three key principles:

- Online behaviours too often fail to meet acceptable standards
- Users can feel powerless to address these issues
- Technology companies can operate without proper oversight, transparency or accountability, and commercial interests meaning that they can fail to act in users' best interests

Home Office and DCMS are now in the process of creating a joint white paper which expected to be published in the winter. The scope of the white paper will include a spectrum of harms, and it will recognise that the UK should be a world leader to encourage the technology sector and provide a stable environment in which innovation and online business models can be successful.

This work falls under the banner of the Digital Charter and is expected to contain a mixture of legislative and non-legislative measures with a view to "future proof" policy. Government will explore a variety of legislative options, including the duty of care suggestion. The release of the white paper will be followed by a period of consultation.

Algorithm Explainer

Ansgar Koene, Senior Research Fellow, Horizon Digital Economy Research Institute - University of Nottingham, explained how algorithms work and the implications for society. He explained the purpose of algorithms is to present vast amounts of information in a format which is much more manageable and accessible for humans.

Services prioritise content in a number of different ways in order to provide a positive and convenient customer experience. Prioritisation can occur on the basis of what you have viewed or liked previously, which content is popular in your community, or which content is viewed by other users with similar demographics to you. This convenience can result in a compromise of control and users do not always know it's happening. The prioritisation of content becomes even more important as space for returning searches becomes limited (e.g. phones) or eliminated in favour of returning one result (e.g. voice-controlled devices).

Algorithms have potential implications for a) bias – in content prioritisation, b) transparency – understanding when algorithms are used and how they decide on content, and c) human agency – as individuals consume content more passively. As filtering using AI is perceived as particularly advanced and cutting edge, some organisations are engaging in 'faux-tomation' – portraying human decisions or human created content as a result of a machine decision making.

Mapping the progress of GDPR and the Data Protection Act 2018

The panel reflected on 2018 as a significant year for data protection legislation. With the EU General Data Protection Regulation incorporated into the new UK Data Protection Act 2018 and the associated public campaigns, we have seen a massive impact on how industry and individuals prioritise and understand data protection.

Panellists

- Nick Wenban-Smith, General Counsel, Nominet (Chair)
- Neil Thacker, Chief Information Security Officer of EMEA, Netskope
- Rosalind Goodfellow, Domestic Data Protection Team, DCMS

The new data protection regime and the promotional campaign in the lead up to 25th May focused industry attention on data protection as a matter of urgency and priority. Supply chains and marketing practices have received particular attention. It also raised awareness among individuals as to the value of their personal data.

The audience questioned whether we would see increased class actions or malicious data subject claims with the intention of paralysing businesses. The panel noted that there are legislative protections to prevent malicious requests and the Information Commissioners Office (ICO) has been given additional resources to regulate. One member of the audience noted having seen calls for individuals to join class actions against Facebook in Brussels. The panel had not seen any evidence of increased class actions so far in the UK.

The panel discussed the implications for data flows following the UK's exit from the EU. Currently, the UK's data protection regime is identical to the EU which indicates that the UK is likely to secure a data adequacy agreement in order to ensure cross border data flows. The government will continue to negotiate on this issue and prepare for all contingencies.

The audience questioned what GDPR means for young people and how it can improve their lives. The panel drew attention to the ICO campaign around information rights and the fact that the GDPR is one part of the government's broader policy work to encourage data literacy in schools. The panel recognised the need to talk about data protection in a way that is engaging, accessible and inclusive of all ages and levels of technical expertise.

COUNTERING DATA EXPLOITATION:
In conversation with Ailidh Callander and Alex Krasodomski-Jones

In this session **Ailidh Callander**, Legal Officer with Privacy International, had a fireside style chat conversation with **Alex Krasodomski-Jones**, Researcher, Centre for the Analysis of Social Media, Demos, on the ethics of selling personal data to third parties, and using personal data for targeted and promoted content.

Ailidh described the wakeup call over the past year and rising awareness of the micro-targeting of personal data for electoral influence. Despite there being data protection laws for twenty years now, it is only the advent of mass data gathering and exploitation which has caused this. In particular, the Snowden and Cambridge Analytica/ Facebook scandals have highlighted the misuse of consent and abuse on a massive scale of individuals' rights.

The enhanced definition of consent for use of personal data under the GDPR was very much to be welcomed, but when analysing the detail of consent and privacy statements this did not match the actual use to which companies were putting the personal data collected. Privacy International has therefore recently filed complaints with the ICO against seven companies active in the markets for behavioural advertising and cross-device data tracking. These included Axiom, Oracle, Equifax and Experian.

The tenor of the conversation was that the additional powers of the ICO under the GDPR were very much to be welcomed and were needed. Whilst individual data subjects were gradually becoming more and more aware of the use to which their personal data was being put, Ailidh stated frankly that she hoped the most data exploitative business models would now be put to an end.

There was some scepticism from the audience that this would actually happen, but no doubt that the landscape has changed dramatically in the past year. It will be very interesting to see the results of the Privacy International complaints as these start to be processed by the ICO.

Lessons learnt from Paris and Dubai

This session reflected on the insights from attendees of the global IGF held in the UNESCO headquarters in the Paris the previous week, and the four-yearly ITU Plenipotentiary Conference held in Dubai on 29th October – 16th November 2018.

Panellists

- Richard Wingfield, Legal Officer, Global Partners Digital
- Mark Carvell, Head of International Online Policy, DCMS
- Desiree Miloshevic, Internet Society UK Chapter Lead Team and Internet Society Board Trustee

Speaking first to the ITU Plenipot, Richard Wingfield, reflected at the growing number of discussions and references to matters which included internet governance. He explained that the ITU had sessions that covered every item for discussion on the UK IGF agenda that day, and the growing desire within some ITU members for multilateral governmental oversight of certain areas of the internet. Whilst there is still much support for the multi-stakeholder model from liberal democracies, in worldwide terms approximately 50% firmly reject this approach.

Resolutions related to Over the Top (OTT) cloud services which cross over national boundaries, cybersecurity and attempts at internet regulation were largely defeated and Richard felt that in that regard the Dubai meeting had been successful.

Desiree Miloshevic, then gave an overview of the Paris IGF held the previous week. In terms of prominence it was the first IGF ever to have been addressed by the UN Secretary General and the host country head of state. President Macron of France made wide-ranging, and in some quarters, highly controversial comments on the role of governments in regulating the internet for the protection of their citizens, and rejected the dominance of the Californian and Chinese models for internet governance. Although the IGF meeting was shorter than previous meetings at only three days, a record number of panel sessions, workshops and dynamic coalition meetings had taken place.

Mark Carvell, continued with a discussion on the future of the IGF with reform very much being on the agenda and advanced both by France and Germany, who are the host for 2019's Global IGF. The perennial topic of the relevance and role of the IGF continues but now momentum seems to be building for increased focus on outputs and tangible recommendations from which policy changes can be formulated. Despite the IGF being in some difficulty in terms of relevancy and the host for 2018 being announced very late – one of the reasons why the UK IGF was held after the global IGF for once, the meeting was extremely widely attended and supported.

Cybersecurity and the internet of things: 'security by design'

Edward Venmore-Rowland, DCMS, introduced the government's 2018 report 'Secure by Design: Improving the cybersecurity of consumer internet of things' report. This was followed with a panel discussion chaired by **Olaf Kolkman**, Chief Internet Technology Officer, The Internet Society.

Panellists

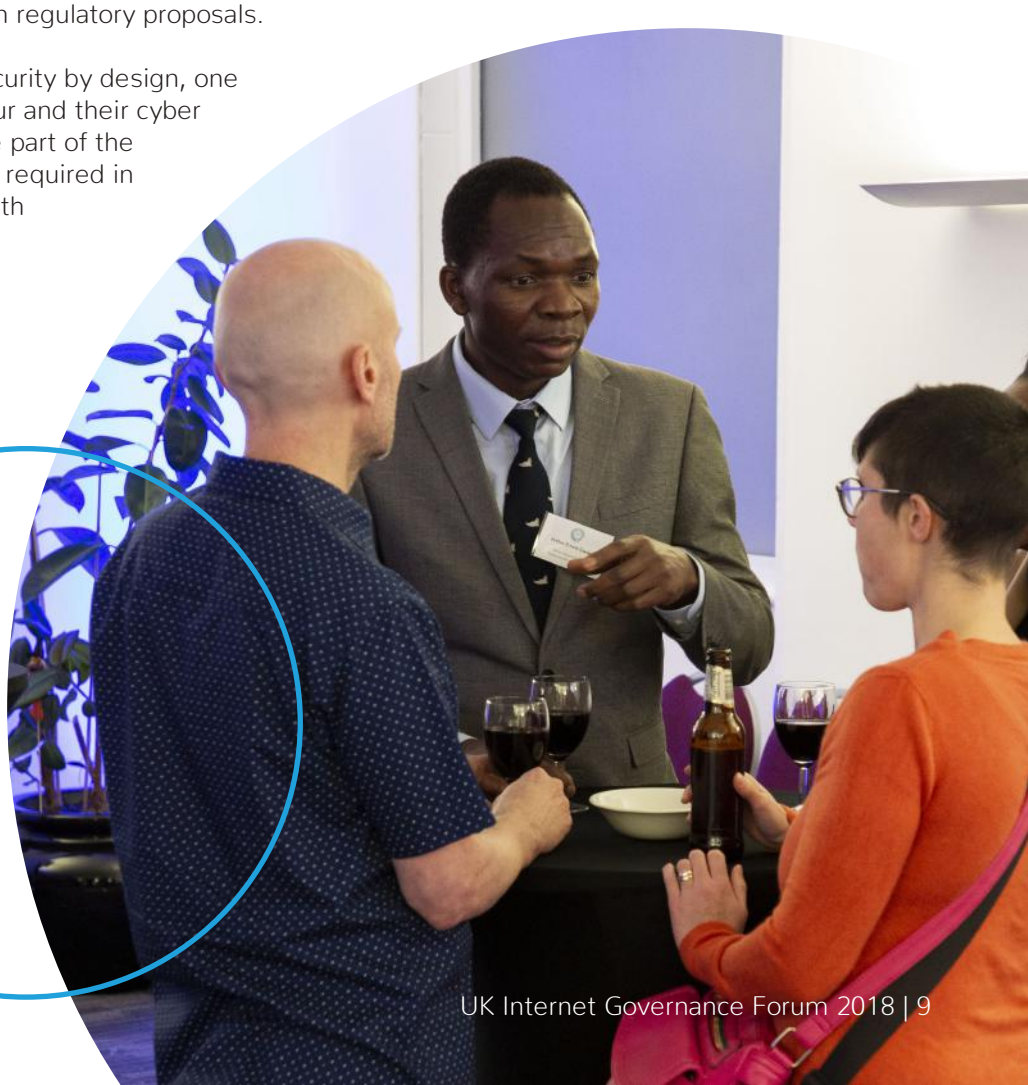
- Talal Rajab, Head of Programme – Cyber and National Security, Tech UK
- Stephen Pattison, Vice President of Public Affairs, ARM
- Eva Blum-Dumontet, Privacy Research Officer, Privacy International
- Matthew Shears, Director of Cyber, Global Partners Digital and Board Member, ICANN
- Joyce Hakmeh, Cyber Research Fellow, Chatham House

The government aims to reduce the burden on consumers by ensuring that security is built by design into IoT devices. Previous consultations have resulted in DCMS Secure by Design reports and code of practice in 2018. Panelists recognised and supported the UK government's efforts to highlight the Code and ETSI Technical Specification with international governments to help create an aligned approach. The rapid growth of the IoT market means that the security of these devices is a present and pressing challenge for government, industry and the public. There was a wide ranging discussion with many contrasting views, which demonstrated the multifaceted and extremely complex nature of the issues. There was broad agreement that a UK Code of Practice was important and necessary, but not sufficient. A theme was the need to work to establish where responsibilities lie and how they relate to each other.

The challenge of squaring consumer preference with security was another theme: security is often not high among people's reasons for choosing a product. One study suggests that 50% of consumers cite security as a key barrier for using an IoT device. But cost is the other big barrier – presenting a challenge to increase security and trust without increasing cost.

Given this, one view was that regulation can set a minimum bar but the tech sector must move fast itself to keep pace with hackers. Industry should endeavor to make devices safe and recognise that security builds trust, and trust is crucial to business. Establishing security cultures across industry and agreed industry standards will be key elements to achieving this. Supply chain challenges are another complex and crucial element, which it was suggested needed to actively feature in regulatory proposals.

Despite the government's focus on security by design, one panellist pointed out that user behaviour and their cyber health could not be ignored. People are part of the ecosystem. A generational shift will be required in how people understand and engage with data and security issues; GDPR has potentially catalysed this shift.



You can keep up to date with the work of the UK IGF by visiting our website at
www.ukigf.org.uk