UK INTERNET GOVERNANCE FORUM REPORT 2021

Wednesday 20th October
and Thursday 21st October 2021

Virtual event

www.ukigf.org.uk

UK IGF

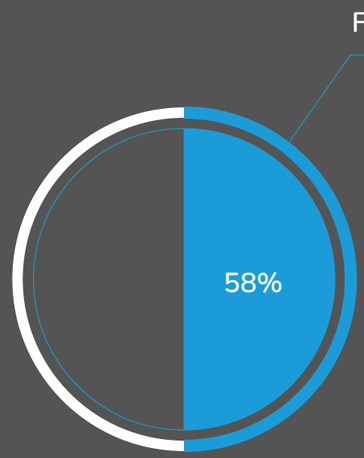
The UK Internet Governance Forum (UK IGF) is the national IGF for the United Kingdom. IGFs are an initiative led by the United Nations for the discussion of public policy issues relating to the internet. A key distinguishing feature of IGFs is that they are based on the multi-stakeholder model – all 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.

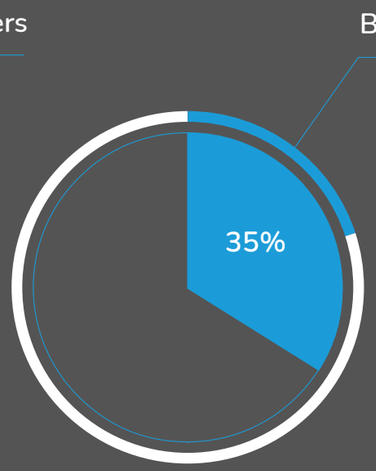
In 2021, as a result of the Covid-19 pandemic, the UK IGF was held virtually for the second time. We learnt from our previous virtual experience and aimed to provide a more focused event with fewer sessions to keep the audience engaged. We also focused on morning sessions as these received higher attendance in 2020, and prevented people having to take a whole day away from vital work and life commitments – which can often be more challenging when you're still sitting at the same desk or in the same location. This is also vital as we continue to prioritise a UK IGF that is inclusive of diverse voices and life circumstances.

From 20th – 21st October, 145 delegates from government, civil society, parliament, industry, the technical community, and academia met virtually to discuss **The Future of the Internet.**

The content was aligned to the five themes: Trust, Inclusion, Data, Environment and Covid-19.

Our speakers were more diverse and better representative of the UK than ever before, with 58% of speakers being female and 35% being BAME. This continues to be central in terms of how UK IGF is designed to ensure the discussions are truly relevant to the experiences of all UK digital citizens.





This report summarises the discussion and provides key messages for consideration at the United Nations IGF and beyond.

The speakers participating in this year's event were more representative of the UK than ever, with 58% of speakers being female, and just over a third Black, Asian and Minority Ethnic (BAME).

All presentations were recorded and are available to watch at **ukigf.org.uk/2021**.

The UK IGF has a steering committee and secretariat. The committee members can be found at **ukigf.org.uk/committee** and the secretariat is provided by Nominet, the UK's national domain name registry.

We would like to thank all those who participated and made the event possible.

If you are interested in contributing to the UK IGF, please contact **info@ukigf.org.uk** you can view our Donor Report at **ukigf.org.uk/donate**.

The 2021 UK IGF was sponsored by Nominet, Donuts, ICANN and ISOC England.

KEY MESSAGES

The past two years have accelerated the growth in the amount of time that UK citizens spend online. The majority of UK citizens have experienced a dramatic shift towards more flexible ways of working, shopping, education and entertainment.

The divide between people who have ready access to the full range of tools necessary for an inclusive and effective online participation has unfortunately also increased.

Even with this growth, future demand for digital services is set to double over the next 10 years, and so better solutions to ensure the whole nation is able to benefit must be found.

Online crime has also exploded, rising to £52 billion losses annually. The next year will see legislative measures being taken to tackle criminal activity online, and protect children from harmful content, whilst protecting free expression online.

WELCOME

Eleanor Bradley, Interim CEO, Nominet welcomed attendees. She also thanked the multi-stakeholder steering committee and the funding providers. In addition to Nominet, the 2021 event was funded by donations from Donuts, ICANN (The Internet Corporation for Assigned Names and Numbers), and The UK Chapter of the Internet Society.

Eleanor noted the work undertaken this year to encourage and champion under-represented voices. The UK IGF has now signed up to the Future of London's Speaker Diversity Pledge and worked with them to ensure speakers are representative of the society we live in. She set out how the multi-stakeholder model in bringing together diverse views on opportunities and challenges of the internet

The Committee also focused on youth participation; 21% of the participants this year identified as aged under 25 – the largest category in attendance. She also welcomed the two-thirds of participants had registered for their very first IGF, outlined the topics of the day and introduced, and introduced the first keynote.

MINISTERIAL ADDRESS

Chris Philp MP, Parliamentary Under Secretary of State at the Department for Digital, Culture, Media and Sport provided the first keynote of the day. He emphasised the importance of topics being discussed, many of which align with UK Government policymaking – such as regulating online harms and the future of the internet.

The Minister emphasised the Government's plans to support the digital economy and remove potential roadblocks to growth. He noted the importance of online safety and regulating in a way that does not stifle innovation, as the government moves forward with their plans for it's Online Safety Bill, indicating that improvements will be made following pre-legislative scrutiny.

The Minster also set out the importance of non-regulatory safety technology, such as age assurance and verification. This sector is growing rapidly, and the government is keen to support its development across the UK. Media literacy is also essential and users need to be empowered to understand and engage with digital media safety. The international aspect is also key; collaboration with partners through networks like the G7 and "five eyes" will be a priority for UK Government in the year ahead.

He also set out some of the objectives of the Government's National Data Strategy; to drive new opportunities and ensure regulation doesn't hamper new ideas and research, while also maintaining public trust.

Finally, the Minister also reiterated to attendees opposition to any efforts that would bring the internet under restrictive government control when looking at the future of the internet, reiterating the Government's support for the multi-stakeholder model of internet governance.

DATA PROTECTION

- Kenneth Cukier, Senior Editor at The Economist, Chair
- Benjamin Mueller, Senior Policy Analyst at the Centre for Data Innovation
- Dr Michael Veale, Associate Professor at UCL
- Sahdya Darr, Immigration Policy Manager, Open Rights Group
- Renate Samson, Principal Policy Advisor, Which?

Kenneth Cukier, Senior Editor at The Economist kicked off the first panel with an intentionally provocative question in his role as Chair – asking if "Brexit the best thing that's ever happened to the UK"? – to open wider discussion of whether the UK's data protection regime should change under its new regulatory flexibility and a data strategy.

Sahdya Darr, Immigration Policy Manager, Open Rights Group advocated for the importance of protecting individual privacy rights. "Privacy is power" she noted, commenting that there is a slippery slope if the government is going to do away with the privacy protections put in place for citizens, particularly for the most vulnerable. Innovation, while welcome, should not come at the expense of privacy and trust.

Dr Michael Veale, Associate Professor at UCL outlined that the GDPR framework has sufficient flexibility to allow for even states bound by EU law to tweak their regimes appropriately. In fact many sensible reforms are possible without rewriting the legislation, and GDPR has been misrepresented. The scope is already there for the UK to provide clarity and targeted leadership without a dramatic conceptual divergence from existing data protection.

Renate Samson, Principal Policy Advisor, Which? noted the opportunity the current juncture represents for additional transparency.

As consumers are at the heart and are the subject of data, they shouldn't be distanced from this integral part of their lives – putting individual rights at the heart of data doesn't prevent innovation and is essential to bolster user confidence.

Benjamin Mueller, Senior Policy Analyst at the Centre for Data Innovation raised some points in support of changing the UK's data protection regime, noting potential benefits of shifting data protection rules away from assessing the means of data controllers' decision making, towards assessing the outcome – which might include uncontroversial benefits for the data subject. He also urged the case for a balanced debate; and to avoid overstating the risks of greater flexibility.

The panel also considered the role of large tech companies and artificial intelligence being used for decision making. They also noted the political economy of data – which usually results in small businesses inserting their data sets into larger companies who get the benefit of the data, while start-ups that legitimately threaten larger companies in the space of AI are simply acquired.

There was a common call for placing individuals and community engagement at the heart of these discussions, to explain, to engage and to help empower people, and put them at the heart of discussions like these.

FUTURE OF THE INTERNET

- Dr Hosein Badran, Director, Internet Growth and Trust - ISOC
- Alain Durand, Principal Technologist at ICANN
- Lise Fuhr, Director General at ETNO
- Alissa Cooper, Vice President of Technology Standards, and a Fellow at Cisco Systems

Dr Hosein Badran, Director, Internet Growth and Trust, ISOC, chaired and opened the UK IGF panel on the future of the internet by looking to its past; asking panellists what the key principles of the internet to date, and why they had made it so successful.

Alain Durand, Principal Technologist at ICANN responded that the number one characteristic of the internet is its openness – that anyone can connect – and that this was more defining of its character that the number of users or its speed. No permissions, gatekeepers, and barriers. If you had to ask permission to connect, the internet would never have happened in the same way.

He also noted that decentralisation is key principle of the internet and core protocols are kept to a minimum to allow independent and interoperable management – which in turn allows for a rapid pace of innovation.

Alissa Cooper, Vice President of Technology Standards and a Fellow at Cisco Systems set out the case for forums like UK IGF to bridge between the technical level of the internet and the political and commercial world.

It's important what is discussed at the technical level is understood by all the normal users of the internet and those setting policy and operating practice. Communication between technical and political stakeholders would be essential to preserve the multi-stakeholder model in future.

Lise Fuhr, Director General at ETNO noted that without trust in the internet, users aren't going to fully utilise it.

It's not that security isn't a good idea, but if you centralise the traffic this can also make it difficult for some operators to comply with legal requirements. For example, compliance with NIS 2 in the EU is made more difficult with some security initiatives, depending on the initiative – giving DNS over HTTPs as an example.

DAY 2

KEYNOTE SPEAKER: OFCOM

Yih-Choung Teh, Group Director, Strategy and Research, Ofcom shared some key findings from two recent Ofcom publications; Ofcom's 'Online Nation' report and it's 'Technology Future's' Report.

In the former, Yih-Choung Teh noted three key findings. Firstly, UK citizens are spending an enormous amount of time online. In 2020, in the peak of lockdown, we spent more than a quarter of our waking hours online, and our streaming time doubled. Second, this reality has increased the harms of the already massive digital divide. 6% of UK households do not have access to the Internet at all. He also noted it is not just about being online, but how we use it. 10% of adults rely on a mobile phone for internet access, which can make some activities challenging.

He also noted that most content is now user generated, and that brings opportunities, and risks of harm too. It has had democratising effect for consumers and social movements, but 70% had seen or experienced something harmful – fake news or offensive language in particular. Children are especially vulnerable, 81% of 12-15 year olds say that they've had a potentially harmful experience in the last year, the most prevalent experience (30%) was being contacted by someone they don't know.

Ofcom's second report, Technology Futures, put a spotlight on the technologies which may influence the internet of the future. Teh noted that adoption curves are getting steeper – and that online behaviour is evolving faster than ever. The internet continues to foster innovation and new players with new propositions continue to grow very quickly, with the emerging concept of the Metaverse attracting attention, and investment.

This has raised questions for regulation and Ofcom's approach as an online safety regulator. For this reason, regulation must be able to adapt and shouldn't take a fixed approach. Enforcement needs to be targeted, transparent and proportionate, to protect freedom of expression, and international collaboration and coordination will be critical. Due to growing number of platforms, the issues are complex, overlapping and interconnected globally.

CYBER-CRIME

- Dr Louise Bennett, Director, Digital Policy Alliance
- Joyce Hakmeh, Senior Research Fellow - International Security Programme at Chatham House; Co-Editor at Journal of Cyber Policy
- Dr Victoria Baines, Associate, Oxford Internet Institute & experienced cyber security professional
- Phillip Donnelly, Detective Chief Inspector & Cyber and Darkweb Technical and Capabilities Lead at the NPCC Cybercrime Programme

Louise Bennett, Director, Digital Policy Alliance, chaired and opened the session, setting the scene of a rapidly rising demand for digital services that will double in the next ten years. For all these opportunities, online crime has also exploded, with £52bn in UK losses to crime. She also noted victims and perpetrators often reside in different jurisdictions, which in turn require a national and global endeavour to tackle.

Joyce Hakmeh, Senior Research Fellow, International Security Programme at Chatham House advocated for the UK to push for transparency and a multi-stakeholder approach in leading the prevention of cybercrime. She explained the UK should invest in capacity building efforts and adopting a strategic approach, it's not just about having a cybercrime law or a cybercrime unit – we need to look at prioritisation and enabling frameworks.

Phillip Donnelly, Detective Chief Inspector & Cyber and Darkweb Technical and Capabilities Lead at the NPCC Cybercrime Programme talked about the UK police approach to cybercrime. There are "four Ps" that guide their approach - Pursue, Protect, Prevent and Prepare. There is an increasingly joined up approach across the UK, and everyone who reports cyber-crime to police will get a call back, a move that is about prevention as well as restitution. However, there is a poor understanding of the threat picture because incidents aren't always reported to police, and often businesses are not aware of how the police could help.

Dr Victoria Baines, Associate, Oxford Internet Institute set out that "cybercrime" means many different things to different entities. To a nation state, it's a foreign state threat, for example. These blurred distinctions matter because it leads to confusion. We therefore need to think about communicating differently to different stakeholder groups on cyberspace – all too often the threat feels "too big, too militarised, and unmanageable".

She noted that despite pessimistic expectations, many millions of us around the world have shown ourselves capable of doing things to protect ourselves and others in the pandemic – it was possible to deploy public health measures against the pandemic, and a public health framework could be applied to cyber threats too.

When asked for top tips on cyber for businesses, the panel noted they should use a password manager if possible, patch systems, and educate staff, be vigilant, have a cyber incident response plan that you practice, and audit – ensuring to remove old employee access, and update legacy software.

GREENING THE INTERNET

- Ana Yang, Sustainability Accelerator, Chatham House
- Emma Fryer, TechUK, Associate Director for Data Centres. Tech UK
- Michael Oghia, Director of Communications and External Relations at the Sustainable Digital Infrastructure Alliance

Ana Yang, Sustainability Accelerator, Chatham House chaired the session on climate change and the internet. Ana introduced the session with a summary of the state of play of climate emergency and the internet entering COP26. She noted that every single sector will need to be mobilised to ensure the globe can remain in an increasingly challenging 1.5-degree threshold for temperature rises. This is looking near impossible unless policies can be deployed "at scale and fast".

Emma Fryer, TechUK, Associate Director for Data Centres responded by asking how the tech sector can respond to an increase in demand without having an increase in emissions? The sector will have to look at efficiency, and to improve transparency and awareness. One key challenge is that freemium services don't give price signals of their emissions impact. This is problematic as it seems a significant number of children don't think the internet uses any energy at all.

Michael Oghia, Director of Communications and External Relations at the Sustainable Digital Infrastructure Alliance, recommended attendees see sustainability as a holistic issue, noting that the idea that digital infrastructure is just data centres isn't right – there is much more, ranging from transportation, software developers and technology providers. We must make the business case for sustainability at every part of the value chain, and those solutions need to be viable to take off.

When asked for their one hope for action, the panel set out their hopes citizens recognise the best is not the enemy of the good, and that they can do what they can do, and not worry about being perfect. This also means thinking locally, even though our problems are global; voting, participating in consultations, can make a difference. They also stressed infrastructure providers shouldn't underestimate the power of their collective procurement power, and request sustainability from their suppliers.

ONLINE SAFETY BILL / ONLINE HARMS

- Professor Victoria Nash, Director, Associate Professor and Senior Policy Fellow - Oxford Internet Institute
- Damian Tambini, Policy Fellow in the Department of Media and Communications at LSE
- Alan Rusbridger, Facebook Oversight Board & former editor of the Guardian
- Orla MacRae, Deputy Director, Online Harms Regulation at DCMS

Professor Victoria Nash, Director, Associate Professor, Oxford Internet Institute chaired the session, noting the prevalence of the Online Safety Bill ahead of this session, due to be tabled in Parliament in the coming months.

Damian Tambini, Policy Fellow in the Department of Media and Communications at LSE, responded that despite reservations the proposed framework is "sounds" like a balanced a structure of institutions and incentives to change behaviours online. The need is there for an iterative approach, but the bill sets initial standards that can grow into a more complex, sophisticated, multi-stakeholder and co-regulatory system.

He urged there to be more work done on the balance of power between Ofcom and the Secretary of State in the new regime, and that Ofcom should be, and be seen to be, independent in it's decision-making, and have no role in content; instead shaping design of services so that platforms reduce harm through their duty of care. It's vital too that this approach is trusted by the public.

Alan Rusbridger, Facebook Oversight Board, explained that at the heart of the challenge is an explosion in communications platforms, that regulators struggle to keep up with. Companies themselves have acknowledged the need for help with oversight. However, these challenges are difficult. They involve looking at global challenges on content with a local context; that means looking at the vocabulary, language and political context used. It would be easy for companies to "over-moderate" – but risks that could be as harmful as "under-moderation".

Rusbridger encouraged policymakers to take a 'global' view, not just a Western one, and a nuance in how freedom of expression is based around the worked. Given that platforms have struggled with their independence in recent years, it's vital Ofcom as an online harm regulator has guarantees of its independence too.

Orla MacRae, Deputy Director, Online Harms Regulation at DCMS, noted that the Government is listening and learning from debates like these, and is aware the Draft Online Harms Bill is leading an international debate on the subject.

Ultimately, Government has three objectives; first to tackle criminal activity online, second to protect children from harmful content; and third to protect free expression online. This is not a choice between one or the other, user protection is not opposed to freedom of speech. Government has a duty to ensure everyone feels able to contribute online while free from harassment. This contradiction is at the heart of a misconception around the Bill, one that is designed to regulate systems and processes, not content.

UK INTERNET GOVERNANCE FORUM REPORT 2021

www.ukigf.org.uk

Thank you to our Steering Committee:

IWF Internet Watch Foundation
DIGITAL POLICY ALLIANCE
Access Partnership
donutsinc
Internet Society UK England Chapter
techUK
NOMINET
ICANN
Department for Digital, Culture, Media & Sport
ARTICLE 19
CHATHAM HOUSE
GLOBAL PARTNERS DIGITAL
ORG OPEN RIGHTS GROUP