

UK INTERNET GOVERNANCE FORUM REPORT 2022

Tuesday 1st November

Hybrid event

www.ukigf.org.uk



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 global public policy issues relating to the internet. A key distinguishing feature of IGFs is that they are based on the multi-stakeholder model whereby 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 2022, after two years of hosting virtual events due to the Covid-19 pandemic, the UK IGF held a hybrid event in London on the 1st of November. We have worked hard to hold an inclusive event for those joining virtually by enabling the chat function and announcing questions submitted online via Zoom. Meanwhile, the in-person event had opportunities to network during the breaks and included a drinks reception in the evening so that delegates could continue discussions held during the day.

On 1 November 2022 we had 120 delegates attend the event with representatives' government, civil society, parliament, industry, the technical community, and academia to discuss this year's theme: Resilient Internet for a shared sustainable and common future.

Diversity continues to be a central part of the UK IGF. A wide range of backgrounds, perspectives and opinions were included in the event design by the volunteer steering committee to ensure the discussions were truly relevant to the experiences of all UK digital citizens.

This is why, for the second year, the steering committee signed the Future of London Diversity Pledge to ensure that the speakers and panels were representative of the society we live in today. The speakers participating in this year's event were more representative of the UK than ever before, with 58% of speakers being female, over 30% from outside of London and the Southeast, and just over a quarter from ethnic minority backgrounds.

The steering committee were also pleased that 71% of delegates that registered to attend did so for the first time, and that there is continued growing engagement from younger delegates.

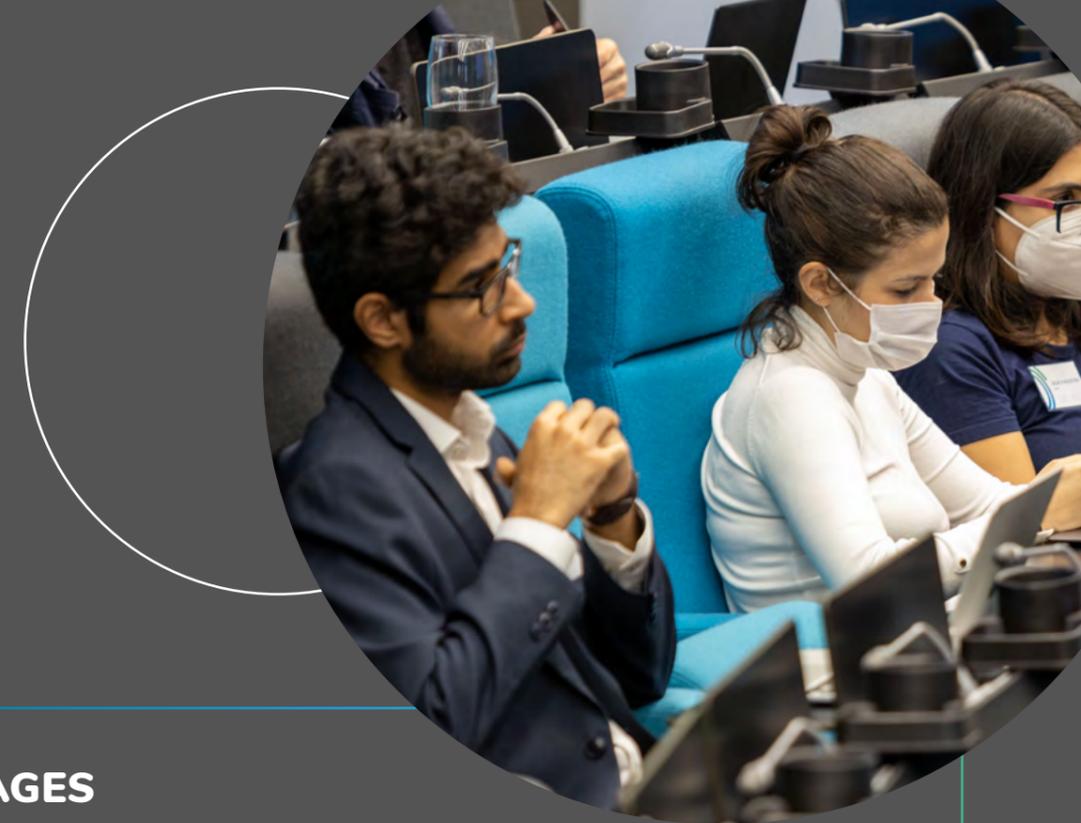
This report summarises the discussions and provides key messages for consideration at the United Nations IGF meeting to be held in Addis Ababa, Ethiopia 28 November – 2 December 2022, and beyond.

All presentations were recorded and are available to watch at ukigf.org.uk/uk-igf-2022-highlights.

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.

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 2022 UK IGF was sponsored by Nominet and ICANN.



KEY MESSAGES

- We are spending an increasing amount of time online, and whilst it holds benefits, it increases our exposure to online harm. It is therefore vital the UK government's Online Safety Bill progresses through parliament before Christmas.
- There is a widening digital divide in the UK, with 6% of people not digitally engaged and a growing number of people relying on smart phones for internet access. It is important to improve digital skills, access and quality of devices to better support people digitally excluded.
- Encryption has a number of benefits, such as enabling private communication, but it can contribute to the sharing of illegal content. Regulators should seek to balance the right to privacy and protect against harmful content, and the UK is developing technologies to facilitate this, such as privacy enhancing technologies.
- Data "is the fuel for the fourth industrial revolution" however trust and transparency through an assurance ecosystem should be considered to utilise the benefits of AI.
- Internet fragmentation is happening, stemming from different ideological and geopolitical goals and focus should be given to how it should be managed. It is important to develop a framework for a free, open and secure internet to prevent other nations being drawn into more oppressive models.
- It is vital that trust and confidence is built across multi-stakeholder groups, as these are ultimately the key fundamental building blocks for resilience and sustainability
- It should be recognised that the themes from UKIGF are all about people, and we should ensure that they remain at the heart of discussions

WELCOME

Nick Wenban-Smith, General Counsel and Head of Stakeholder Relations welcomed attendees and introduced Nominet.

Nominet is the .UK Registry, responsible for domain names that end in .UK. .UK remains the country's domain of choice and Nominet is focused on ensuring its service and policies evolve, not simply to keep pace, but to set an industry standard in the years to come.

Nominet is a Public Benefit organisation, and a large part of this work is protecting public services with Protective Domain Name Service Solutions. Nominet however is committed to going further. Over the next three years, Nominet will spend around £65 million to support partners and programmes that promote greater connectivity, inclusivity, and security.

This includes

- A digital skills, education and training programme with the Institute of Coding.
- Funding the work of the UK Safer Internet Centre (UKSIC), including Safer Internet Day.
- Partnering with the Internet Watch Foundation to develop new approaches to identify and stop the most serious child exploitation and remove inappropriate material from the open web.
- Launch of the second Digital Youth Index, which is a benchmarking report that offers insight into young people's digital experiences, and aims to inform debate, our own funding, and that of our partners.

Mr Wenban-Smith thanked the multi-stakeholder steering committee for contributing their time and expertise throughout not just the day but the months leading up to the event. Lastly, Mr Wenban-Smith thanked ICANN, this year's funding partner.



Lucy Powell, Shadow DCMS Secretary of State & Labour MP for Manchester Central

Ms Powell thanked the organisers for the UK IGF and began her address by providing an overview of Labour's position on Online Safety and Digital Harms. She stated that the digital era has been marked by a concentration of power in the hands of tech giants, who have great amounts of influence over what we buy, how we live and how we think. Labour is looking at the balance of power between people and platforms, as well as the need for a clear framework on the use of data. Ms Powell added that internet resilience is drawn from its users, and that regulation is at the heart of both resilience and competitiveness, because "to win the race, players need to know the rules". Ms Powell outlined Labour's policy priorities in this space, which include developing a digitally connected society and ensuring that a truly resilient internet is open to all, without physical or social barriers to connectivity.

Ms Powell turned her address to the UK's failure to tackle digital exclusion, which she stated was hampering the UK's economic development. According to Ofcom, a third of households are struggling to pay for their broadband and 97% of low-income families are missing out on the social tariff. This is why Labour announced a three-point plan to tackle the costs of broadband:

1. Regulate wholesale price increases by cost not Consumer Price Inflation
2. Ofcom should take action on mid-contract price rises, early termination costs and loyalty penalties
3. The industry should come together to develop a mandatory, well-advertised social tariff for low-income families

Ms Powell stressed she opposes any further delay to the Online Safety Bill as there have already been over 10,000 hate crimes reported online in the UK in the five years since the Bill was first introduced. She stated that if the Bill does not reach the Lords by Christmas, then it could run out of time and although the new Secretary of State has stated that she wants to substantially rewrite parts of the bill, "we mustn't let perfection be the enemy of the good".



ONLINE SAFETY

As a new Government inherits the pivotal Online Safety Bill, the purpose of this panel was to think about its future, and what changes it may undergo in the coming months as the Prime Minister begins to carve out his own regulatory landscape. Panellists discussed the impact that the Bill will have on the industry, and what the response may look like.

Damian Collins MP opened the session as Chair of the panel outlining his contributions to the Online Safety Bill to date. He specifically highlighted the issue of AI driven recommendation tools, and the very serious, even life-threatening harms that these can cause. The inquest into the death of 14-year-old Molly Russell, who died from an act of self-harm while suffering from depression, had tragically illustrated this problem. He recognised there is an ongoing debate on age verification: whether it can be successful and how age verification could be implemented. Lastly, he responded to concerns that loot boxes have been excluded from the Online Safety Bill, however he provided assurance that the government were drafting proposals to bring loot boxes within regulatory scope under the Gambling Act 2005.

Jon Higham began his comments by announcing that Ofcom will be publishing a consultation on how to regulate the online space, including a draft Code of Practice, once the Online Safety Bill has received Royal Assent. This is currently assumed to be in Spring 2023. In addition, Ofcom is intending to consult on age verification and additional safeguards after secondary legislation is introduced. Mr Higham recognised there were a number of intersections between the work of the Competition and Market Authority, Financial Conduct Authority and Information Commissioner's Office in regulating the digital space. This is why Ofcom have created

- Damian Collins, former Minister for Minister for Tech and the Digital Economy, and former Chairman of the Joint Committee on the Online Safety Bill
- Sharon Gaffka, Love Island Season 7 contestant and online harms campaigner
- Jon Higham, Online Safety Policy Director, Ofcom
- Parven Kaur, Founder of Kids N Clicks

a Digital Regulators Forum to ensure all regulators can jointly discuss and respond to existing and emerging online challenges.

Sharon Gaffka highlighted the daily online harassment she faces as a celebrity figure and women with mixed race heritage. She stated that the anonymity that being online provides prevents accountability in people's actions and words, which is why she believes the Online Safety Bill is an essential safeguard for a modern digital society. Ms Gaffka shared her frustration that social media platforms are often reluctant to take obviously abusive and harassing content down, and that this experience has been shared with her by many young people as part of her activism work.

Parven Kaur opened her comments by commending the Online Safety Bill for introducing the criminalisation of cyber flashing and banning illegal material online, however she added that there are still gaps in the bill in terms of child protection. She raised the concern that there is a large amount of grey area under content considered legal but harmful, and that the National Society for the Prevention of Cruelty to Children (NSPCC) research had identified that children who viewed this content have a high level of anxiety, and low levels of self-esteem. She opposed the proposed implementation to allow platforms to regulate what is considered legal but harmful as this would allow platforms "to mark their own homework".

FUTURE OF THE INTERNET

- Sonia Livingstone, Lead consultant for General Comment 25 on the UN Convention of Rights of the Child
- Jessica Barrett, Youth Speaker and Voicebox representative
- Lizzie Coles-Kemp, Royal Holloway University
- Sally West, Policy Manager, Age UK
- Cliff Manning, Research and Development Director at Parent Zone

This panel brought experts from all generations together to host an open discussion about digital inclusion, inequality and their individual experiences of the online world. Nominet's Digital Youth Index was also being used to steer discussions on the reality of the online world for young people, with panellists aiming to unpack its findings.

Chair of the panel session, Sonia Livingstone, asked the panellists what they identified as the main barriers facing the young and the elderly in the digital world. To begin the conversation, she outlined statistics from Ofcom that she felt were important to the debate. These included that this year 99% of young people (16-24) use the internet at home, compared to 73% of 75-year-olds and over.

Cliff Manning raised the concern that online access is increasingly connected to poverty, as the Digital Youth Index highlights. 26% of children and young people do not own a laptop or computer. He raised the importance of the quality of the device, as this also impacted online access. Mr Manning highlighted that there are good social tariff schemes available, but they can be impacted by onerous bureaucracy and organisations should do more to make access easier.



Jess Barrett, in reading the Digital Youth Index report, found that developing digital skills is more challenging than gaining digital access. She raised the importance of teaching parents as well as children to be digitally resilient, particularly regarding online harms, and that young people shouldn't be placed in a position as the "digital lead" in the family. This is because young people can sometimes lack the life experience and critical thinking required to be able to fulfil this role effectively.

Lizzie Coles-Kemp stated that digital access is not a level playing field, and that there are different qualities of accessing the internet. For example, limitations of access by borrowing someone's phone. She encouraged greater sensitivity to people's lifestyles, for example through research and testing, to increase quality digital access.

Sally West said it's really important that people who are unable to get online or are not interested in using the internet should still be able to access critical services. Age UK have found that an increasing amount of people are finding life difficult as services such as banking and booking GP appointments move online, and that this requires them to rely on other people. She urges organisations to consider this and provide better support for the digitally excluded.

KEYNOTE SPEECH

 Yih-Choung Teh, Group Director for Strategy and Research, Ofcom

Mr Teh presented the results of Ofcom's 2022 Online Nation report and more recent research discussing the findings, touching on the themes of this year's UK IGF panels.

He began by stating that for most people in the UK, being online is an integral part of daily life and allows us to connect with others in ways we wouldn't be able to offline. We already benefit from a breadth of online services, and there is much to look forward to. However, Ofcom research tells us that whilst there are benefits to being online, there are also negatives.

So, what does it mean to be an Online Nation?

Mr Teh noted that we are spending a large amount of time online, an average of four hours a day in September 2021, across a variety of platforms. Across the different age groups 18–24-year-olds continue to spend the most amount of time online at just over five hours, compared to those aged over 55, who at three hours spend the least. We are “increasingly a smart phone orientated nation,” because of the time we spend online, three quarters is now via a smart phone.

Increased smart phone reliance exposes the digital exclusion reality in the UK. If you are a younger person or have a lower socioeconomic background, you are more likely to have to rely on a smart phone for internet access, and this has its limitations. In addition, 6% of households in 2021 had no internet access in their homes which could be because of data poverty, lack of digital skills or lack of interest.

He stressed that it is Ofcom's mission to make communications work for everyone; “We want to see opportunity and choice for all”. In preparing for new responsibilities to tackle online harms, Ofcom has undertaken further research which found that 6 in 10 people reported at least one instance of harmful behaviour or content they had seen recently.



One of the most obvious instances of online harm is stumbling across violent video content, which can be termed an isolated exposure to a hazard. Ofcom has learned that experiencing more severe harm can be linked to cumulative exposure; passively absorbing social media content for example about body image, consistently over time. Cumulative active exposure to certain channels, for example pro anorexia forums, can self-reinforce and cause more significant and severe harm than an isolated exposure.

He drew his presentation to a close by outlining Ofcom's ongoing areas of focus: online safety, digital markets, and media literacy.

1. Ofcom expects industry to respond to online safety issues, such as challenges with emerging immersive technology, data privacy and scams by taking responsibility, providing tools and a growth in the safety technology industry.
2. Digital communications should work for everyone and should have greater investment. Ofcom will be considering regulation in digital markets promoting competition whilst protecting people.
3. Greater investment in media literacy is vital to stay safe online with emerging technology but to also encourage the skills and confidence to flourish.

ENCRYPTION

- Alec Muffet, Led the team that added end-to-end encryption to Facebook Messenger
- Dan Sexton, Chief Technology Officer, Internet Watch Foundation
- Stephen Bonner, Executive Director for Regulatory Futures and Innovation, Information Commissioner's Office

Alec Muffet provided an overview of encryption, highlighting it as an example the development of Global Positioning Software (GPS) and its many great advantages (not least, Pokemon Go!). He raised the importance of securing digital environments but added that everyone has different threat models. Mr Muffet raised the fundamental importance of trust in underpinning a secure digital environment.

Dan Sexton opened his comments by highlighting the importance of secure encryption for a functional internet, but that it can be misused, particularly in the sharing of illegal content. He recognised that the challenge for regulators is how to balance the privacy of communications but stop harmful content. Mr Sexton stated privacy is a right, but not an absolute right if it contributes to harm.

Stephen Bonner began by stating that one of the ICO's core objectives is to improve cyber security, including encryption. He strongly believed that there are mechanisms that can be introduced which protect the privacy of communication but can also highlight and protect against harmful content. An example of this would be preventing those aged 13-15 from receiving direct messages on an online platform, and for those aged 16-18 enabling users to accept or decline messages. Mr Bonner raised the benefit of privacy enhancing technologies that can identify patterns of behaviour, without impacting privacy, that can cause harm e.g password security.



TRANSPARENCY AND AI

- Stephen Metcalfe MP, Chair of Parliamentary and Scientific Committee
- Dr Evert Haasijk, Artificial Intelligence Expert and Senior Forensic Manager, Deloitte
- Bridget Boakye, AI Lead, Tony Blair Institute

This panel discussed how to ensure that the datasets collected by governments, advertisers, and businesses through AI and Machine Learning are transparent to the users whose data they have collected. In addition, the panel discussed how inaccurate data can lead to biased decision-making, and the impact this can have on trust

Stephen Metcalfe MP introduced his work as Co-Chair of the All-Party Parliamentary Group on AI to define AI and identify the challenges and opportunities. He noted that throughout the work of the APPG, he has found that everything is underpinned by data and that "data is the fuel for the fourth industrial revolution". This poses several questions, such as: whether enough people know that their data is being collected, how it is being collected and why? Mr Metcalfe recognised that data can be misused creating unintended bias or intended bias and urged for greater scrutiny.

Ms Boakye began her comments by expressing that that we need to deliver AI responsibly for citizens and noted that the onus should not only be placed on technology users to understand how their data is being used or misused. This is why transparency is so important, as it can lead to greater user empowerment and understanding about where and how their data is being collected. In addition, how it can be used to inform AI decision-making, which algorithms

are being used and how they are being tested. She noted that there are low levels of trust in, and acceptance of, big-tech and government agencies collecting data. To tackle this, an assurance ecosystem should be introduced, building a model in which those who collect data are also delivering the standards of how data should be used.

Dr Haasijk outlined how he applies AI to combat financial crime in his current role at Deloitte. He recognised that applying AI does hold risks if there is bias in decision-making, which is why working with governments to ensure AI is being applied responsibly is so crucial. In doing so, data-driven decisions can be made with appropriate data, and hidden bias can be analysed and identified. He called for transparency across government, the private sector and other organisations about decisions to automate, the rationale of data collection and what people can do to address any errors made.



AVOIDING INTERNET FRAGMENTATION

- Marjorie Buchser, Executive Director at the Digital Society Initiative, Chatham House
- Akos Erzse, Senior Manager for Public Policy at BitOasis and co-author of *The Open Internet on the Brink: A Model to Save Its Future*
- Margot James, Executive Chair of WMG at the University of Warwick and former Digital Minister
- Scott Malcomson, Author of *'Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web'*
- Emily Taylor, Associate Fellow at the International Security Programme at Chatham House

A number of recent UK government proposals have departed from the 'one internet' framework, raising questions about how committed the UK is to the multistakeholder model of internet governance. This panel discussed these attempts to fragment the internet, as well as what can be done about it, and what role the UK internet governance community can play in promoting a united approach.

Margot James opened the session as Chair of the panel by speaking to the importance of discussing internet fragmentation and that in hindsight, the government she served could have done a better job in responding to this issue. Ms James had been inspired by the United Nations Global Digital Compact that addresses the main threats to ever increasing fragmentation and emphasises the centrality of greater global cooperation amongst countries and organisations.

Scott Malcomson outlined several factors that could help safeguard a borderless internet. Firstly, large technology platforms (e.g Facebook) like the access they currently have to other networks; it is beneficial to cyber

espionage and valuable for the preplacement of cyber weapons and propaganda outside of physical boundaries. Secondly, the borderless internet has facilitated many aspects of globalisation from high-speed currency trading to sub-contracting, which in turn has made it possible to bring hundreds of millions of people out of poverty and created new industrial powers. Thirdly, a borderless internet has also enabled aging societies to combat stagnation by protecting returns to financial capital invested abroad and intellectual capital. Fourthly, with advances in the taxation of e-commerce, nation states are becoming more amenable to the concept of a borderless internet. Similarly, the gradual acceptance by tech multinationals of data mobilisation could make a borderless internet more likely to last. Fifthly, the desire of smaller tech economies to have an economic future should evolve in favour of a relatively borderless internet, because if smaller economies focus only on their domestic economies their revenue potential is subject to an intrinsic ceiling, which has tax and funding implications for them. As a sixth factor, most tech multinationals want to reach

as many markets as possible. As builders and maintainers of most internet infrastructure, they have a very strong motivation against fragmentation.

Lastly, the multi-stakeholder community in internet governance is a good defence against state capture, and an increasingly global culture should act as a barrier to fragmentation.

Marjorie Buscher reflected on how this debate has evolved and challenges of the fragmentation of the internet. She raised the concern that if liberal democracies could not agree on a normative framework for a free, open and secure internet, then other nations might be drawn into more oppressive models. She stressed that we need to create a framework based on democratic principles, however we are still in fierce debate about key issues such as privacy and freedom of expression, how these principles can be transposed to online spaces/cyberspace, and where and how to best protect them. She concluded that if we oppose fragmentation then we should seek to propose policy alternatives in which the internet remains open whilst allowing for developments in other areas of the world.

Akos Erze recognised that it may be optimistic to avoid internet fragmentation entirely and that we should turn our focus to the mechanisms to manage a fragmented internet. He commended the

UK on appointing a dedicated tech envoy and implementing three capabilities: first, staying ahead of technological change and its impact on international and domestic dynamics; second, having the capacity to draft coordinated domestic policy positions with multiple stakeholders; and thirdly, creating unified and consistent footfall in the international space. These capabilities may enable the UK to implement a clear strategic vision in line with its interests and combat a fragmented internet.

Emily Taylor began by stating that the internet is a complex ecosystem and that any network will pull apart and push together. She recognised that many stakeholders have the incentive to retain/safeguard a free, open and secure internet, however, there are also forces for fragmentation stemming from different ideological and geopolitical goals. She noted regulation, sanctions and trade wars could be driving fragmentation faster. In the example of China, this triad of regulation, sanctions and trade tensions could result in irreversible change in its internet landscape; recent developments in China's microchip manufacturing industry may demonstrate these tensions in action. Ms Taylor recognised that multi-stakeholder governance was "less beautiful in implementation that it is in concept" and that the UK should help key stakeholders re-discover the idealism behind a free and open internet".

UK INTERNET GOVERNANCE FORUM REPORT 2022

www.ukigf.org.uk



Thank you to our Steering Committee:

