UK INTERNET GOVERNANCE FORUM REPORT 2023

Tuesday 11th July

Hybrid 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 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.

The UK IGF held a hybrid event in London on 11th July 2023 with 185 representatives from government, civil society, industry, the technical community, and academia to discuss this year's theme: the Internet We Want – Empowering all People.

We 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.

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: 60% were women, there were no all-male panels, 25% were from ethnic minority backgrounds and three were youth speakers.

The Steering Committee were also pleased that 50% of delegates that registered to attend did so for the first time, and we have seen record attendance of younger delegates, with over a third under the age of 34.

This report summarises discussions from the UK IGF and provides key messages for consideration at the United Nations IGF meeting to be held in Kyoto, Japan on the 8-12th October 2023.

All presentations were recorded and are available to watch at UK IGF 2023 Highlights - UK IGF.

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 2023 UK IGF was sponsored by Nominet and ICANN.

KEY MESSAGES

- It is vital that a diverse range of stakeholders are active in shaping the future of Internet governance, strengthening and preserving the multi stakeholder model via participation in the IGF processes (such as at the Global IGF in Kyoto) and through the Global Digital Compact, the Summit of the Future and the WSIS + 20 Review.
- The evolution and widening use of AI raises important questions about the control individuals have over the collection and use of their data by a range of entities, an individual's ability to challenge unfair use and how personal privacy is safeguarded through data protection law. It is important to understand what machine learning models can memorise about data sets, and we must remember that automated decision-making is never free of bias and discrimination.
- In an era of increased geopolitical competition and conflict between superpowers, governance of cyberspace is central to enabling individuals to rise above conflict and have full access to their rights and freedoms. We need to use, collect and share data in a responsible way, and increased international multilateral cooperation could help ensure fair and justifiable access to all and limit barriers to a truly global Internet.
- As we live in a society with a pluralistic value set, Internet fragmentation at all levels of the Internet is unavoidable. Technical fragmentation is most detrimental because it could impede the benefits of a free and open Internet, however the practical challenges of Internet governance should not be underestimated, particularly for organisations trying to service multiple Internet governance bodies alongside engagement with national governments. Wider society must be involved in shaping the Internet because we are creating the future of how we communicate with each other and our future shared values.
- Embracing the opportunity of digital transformation is about ensuring good access to reliable digital infrastructure and developing a deep understanding of what digital capabilities are needed to respond to transformative social political shifts, identifying the gaps and creating the right environment to upskill and reskill appropriately.
- the Internet should and has the potential to be a safe space for people with diverse gender identities to freely express themselves, however the Internet has been weaponised to spread discrimination and hatred. Focus should be paid to centring gender perspectives in policymaking and governance, particularly on AI-generated images and introducing greater transparency amongst large technology companies.

WELCOME FROM NOMINET

Ellie Bradley, MD Registry & Public Benefit, Nominet

Ellie Bradley, Managing Director of Registry and Public Benefit at Nominet, opened the eighteenth UK Internet Governance Forum. Nominet is the public benefit organisation responsible for domain names that end in .UK.

Ms Bradley provided a history of the United Nations (UN) World Summit on the Information Society (WSIS) and the importance of engaging in the upcoming review (WSIS +20) in 2025. This review could mark a change to how the Internet is governed as there are an increasing number of countries that want to see greater government involvement in charting the Internet's future.

The UN will also hold a 'Summit of the Future' to reinvigorate and further develop multilateral frameworks in 2024. A Global Digital Compact is proposed as part of this Summit, and is due for negotiation this year and next.

How Internet governance evolves to meet the challenges of the Internet now and in the future is a critical debate, but one that needs to build on the principles and success of the multistakeholder model.

Ms Bradley concluded that it is therefore important that national IGFs, such as the UK IGF, are active participants in shaping the debate at not just the Global IGF but by engaging with the Global Digital Compact and WSIS+20.

TECHUK TECH PLAN: HOW THE NEXT GOVERNMENT CAN USE TECHNOLOGY TO BUILD A BETTER BRITAIN

Neil Ross, Associate Director of Policy, techUK

Mr Ross introduced techUK and the Tech Plan, which sets out how a government can seize the benefits of technology to ensure Britain remains at the global forefront of innovation.

The UK has a strong and dynamic tech market, but the pace of our delivery has faltered in recent years. There has been a lack of long-term planning by the government, failure to deliver key tech strategies and a confused approach as to whether the UK should align with - or diverge from - the European Union (EU).

techUK have identified five challenges to overcome to become a global tech leader. The UK should seek to

1. Improve skills and adoption;
2. Address the scale up challenge;
3. Become more competitive for investment;
4. Improve the procurement of technology into government and public services; and
5. Seek to improve access to data.

techUK have identified eighteen opportunities to overcoming these challenges through a constructive partnership between the tech sector and the next government. Notably, a £5.69 billion pay rise for British people could be achieved by providing increased options and support for people to reach their potential with new digital skills. Setting out a plan for how the National Health Service (NHS) can buy and integrate technology across its services could modernise the service and ensure it is interoperable with care in the community. In addition, data sharing initiatives and developing an approach to AI ethics, governance and regulation that is able to flex and adapt as the technology itself evolves hold significant opportunities for the UK.

techUK looks forward to working with the sector to put tech at the heart of the solutions to our greatest challenges and to solidify the UK's position as a tech leader.

techUK's Tech Plan can be found at **https://www.techuk.org/resource/a-uk-tech-plan-how-the-next-government-can-use-technology-to-build-a-better-britain.html**

DATA PROTECTION IN AN AI-DRIVEN WORLD

- Lord Allan (Chair), Member of the House of Lords and Former Director of Policy at Facebook
- Abigail Burke, Policy Manager, Data Protection, Open Rights Group
- Dr Ana-Maria Cretu, Senior Researcher in AI and Data Protection, Imperial College London
- Georgia Osborn, Senior Research Analyst, Oxford Information Labs and Research Community Manager, DNS Research Federation

As artificial intelligence (AI) evolves and becomes used more widely, it increases the ability of companies to use personal information in ways that can compromise privacy and data protection. With the Information Commissioners Office (ICO) having updated its guidance on AI and Data Protection in March 2023, this panel discussed the potential impacts and risks that the evolution of AI poses to data protection, as well as potential forms of governance on AI.

Chair Lord Allen opened the panel by asking: what is the importance of the data protection law for AI and how proposed changes to the Law may impact its evolution?

Ms Burke recognised that AI has exciting potential to improve the human condition, but it can cause harm as algorithms can replicate and exacerbate patterns of discrimination and bias in society due to poor quality data. Data-driven automated technologies have a serious impact on people's lives and require serious safeguards through data protection law. This is because it provides people with important controls over the collection and use of their data by private companies and the government, and it also gives them the right to understand and challenge automated decisions.

Ms Burke raised concern that the proposed Data Protection and Digital Information Bill may weaken current Data Protection Law as companies will have more rights to deny consumers access to their data.

Ms Osborn outlined the challenges the EU have faced developing the AI Act in defining what AI is, and how to future proof the definition. The EU AI Act aims to strengthen Europe's position as a global hub of excellence in AI by implementing a classification system to determine the level of risk. Ms Osborn noted that extraterritorial nature of the EU Act will impact the UK and identified an emerging challenge between current UK Data Protection Law and the EU AI Act regarding the use of special category data (characteristics such as ethnicity, sexual preferences and gender). This is because the EU is seeking to regulate against bias in AI, permitting AI developers to process special category data in their models, to ensure monitoring, detection and correction of bias for high-risk AI systems.

Dr Cretu described the technical challenges in measuring privacy risks in machine learning models and generative AI that may impact Data Protection Law. She stated that whilst machine learning models should perform well without memorising personal data it is crucial for protecting privacy that we understand what models can memorise. It is technically challenging to trace individual records in the data training set, so it can be difficult to understand what the model does and doesn't remember. A solution is to study models in a post-hoc situation by developing inference attacks, thinking about the motives of potential untrusted entities and what they would be seeking to extract from a dataset, and applying a technique to see whether sensitive attributes of individual data could be obtained from access to a machine learning model alone. Dr Cretu work at Imperial College London will help build understanding of the possible extraction of sensitive data from a model and how it could be weaponised.

Dr Cretu noted that whilst generative AI models are trained to generate data resembling the training set, she cautioned that they can still be vulnerable to extracting private records depending on the source of the training data.

GOVERNANCE OF CYBERSPACE DURING TIMES OF GEOPOLITICAL INSTABILITY

- David Carroll (Chair), Managing Director, Nominet Cyber
- Bojana Bellamy, President, Centre for Information Policy Leadership
- James Shires, Senior Research Fellow in Cyber Policy, Chatham House

This panel discussed Russia's recent proposal for a Convention of the UN on Ensuring International Information Security and the ongoing Cybercrime Convention negotiations which are due to conclude in February next year. The panel also considered the governance of cyberspace in war, particularly cyberspace as a form of warfare.

Chair Mr Carroll gave an overview of geopolitical challenges that may contribute to the bifurcation or splintering of the Internet as predicted by former CEO of Google, Eric Schmidt and former CEO of the UK National Cyber Security Centre Ciaran Martin.

Mr Shires highlighted five changes in the geopolitical landscape that have implications for the governance of cyberspace and cybersecurity. The first is a renewed threat of serious conflict between global superpowers, namely the Russian invasion of Ukraine. The second is an increasing state of geopolitical competition. Trade barriers often exist for national security reasons however this is becoming blurred by the desire for economic security in a landscape of increased economic competition. Thirdly, there is increased instability in developing countries limiting the access and benefits of technology. Fourth, the increase in climate change risks and lastly, the challenges in the information space for example misinformation, disinformation and the right to education on media literacy.

Mr Shires concluded that the governance of cyberspace is central to enabling countries to either stay out of - or minimize - levels of competition and conflict, and to enabling individuals to have full access to their rights and freedoms.

Ms Bellamy described the benefits of data and that it should be considered an asset to be utilised responsibly within government strategies on cyber security and AI. Ms Bellamy noted that as governments have realised the power of data, there has been movement to limit or prevent the sharing of data outside of its borders. To combat data barriers, Ms Bellamy advocat for international multilateral cooperation to forge a 'new deal for data' to ensure fair and justifiable access to all and limit barriers to a truly global Internet.

BUILDING THE EVIDENCE BASE FOR ONLINE SAFETY

- **Ian Macrae, Director of Market Intelligence, OFCOM**

Ofcom has been gearing up for the last couple of years to take on the role as the UK's online safety regulator, with the much-delayed Online Safety Bill now set to be enacted in the autumn.

A key aspect of these preparations has been building the evidence base to understand the landscape of online safety – the harms that adults and children are exposed to and their impact, the risk factors associated with services and the safety measures that can be employed.

Mr Macrae outlined three pillars that have been developed to understand the online safety system. The first, understanding harms, is monitored through the prevalence of potential harm through Ofcom's Online Experience Tracker. Harm is defined as content harm (harmful images, videos, audio or text), contact harm (behaviour such as trolling, unwanted sexual messages and bullying, abuse or threats) and commercial harm (content or behaviour which puts a user at risk of financial harm or disadvantage). Research from September 2022 identified that in the last four weeks, 62% of adults and 68% of teenagers encountered harmful content or behaviour on the Internet.

The second pillar for building an evidence base for online safety is understanding services. Ofcom's research identified that most adults spend four hours a day on average online but on a small number of platforms. The most harm is often encountered on major user-to-user platforms and big platforms are driving traffic to smaller, higher-risk platforms.

The third pillar is understanding safety measures. Ofcom research found that 62% of people have taken some form of action when encountering harm however only half received a response from the platform. Research across thirty-five platforms found a wide range of safety measures such as the ability to self-report, age restrictions, use of AI to filter content and content warnings.

Mr Macrae concluded outlining the next steps following the Royal Ascent of the Online Safety Bill by Ofcom. Phase one will be to focus on illegal harms duties, the second will focus on child safety duties and pornography and the third transparency, user empowerment, and other duties on categorised platforms.

AVOIDING INTERNET FRAGMENTATION AND CREATING A SHARED DIGITAL FUTURE

- **Casey Calista (Chair), Tech Public Affairs Lead, H+K Strategies and Labour Digital Chair**
- **Izaan Khan, Data Protection Analyst, NOW: Pensions and ISOC YSG**
- **Till Sommer, Head of Policy, Internet Services Providers' Association (ISPA UK)**

With the Global Digital Compact due to be agreed at the Summit of the Future in September 2024, this panel discussed how we might avoid Internet fragmentation and instead work together towards the idea of a shared, open, free and secure digital future for all – which the Global Digital Compact will seek to outline in its own principles.

Mr Sommer opened the debate by stating that there has never been a truly universal Internet. It is more likely there has been an impression of singular global Internet but and as it has become more important, fractures and tensions have become visible. This may stem from a United States (US)-centric development of the Internet encountering friction with different norms and values that other parts of the world may hold.

Mr Sommer noted that the expense and time pressures of attending multiple Internet governance bodies discussions whilst balancing engagement with national government is challenging. This becomes more difficult if you are a single-issue organisation as, to have an impact, you may have to engage with multiple complex discussions.

Mr Khan noted that fragmentation exists in multiple layers of the Internet including at the technical, user experience and governance layers. He recognised that as we live in a society with a pluralistic value set, fragmentation is unavoidable however the most detrimental is fragmentation at the technical level, as this could impede the benefits of free and open access to information. Mr Khan also outlined the counterpoint that in some cases fragmentation may be beneficial, resulting in geo-localisation and linguistic diversity.

Mr Khan stressed to the importance of engaging with the Global Digital Compact to strengthen and preserve the multistakeholder model of Internet governance. Mr Khan advocated for the Internet Governance Forum Plus model which would develop policy messages and take actionable discussion to the relevant bodies. Mr Khan argued that the UN proposal to create a new forum (to co-ordinate separate Internet governance bodies, i.e. the Digital Cooperation Forum) could have the unintended consequence of increasing fragmentation at the governance level.

Ms Calista concluded on the importance of increasing accessibility within Internet governance bodies and encouraging the involvement of wider society. This is because we are creating the future of the Internet, the future of how we communicate with each other, and future shared values.

GENDER AND THE INTERNET: A SOURCE OF DIVISION OR COMMUNITY?

- **Professor Katharine Millar (Chair), Assistant Professor of International Relations, London School of Economics**
- **Seyi Akiwowo, Founder and CEO, Glitch**
- **Dr Bernie Hogan, Senior Research Fellow, Oxford Internet Institute**
- **Mallory Moore, Independent Researcher, Trans Safety Network**
- **Isabella Wilkinson, Research Associate, Chatham House**

On the Internet, people with diverse gender identities have created safe spaces and opportunities for freely expressing themselves. Around the world, the Internet is a tool for advancing gender equality through empowerment, learning and organizing.

However, the Internet has also been weaponized to spread discrimination and hatred. Political discourse has recently been dominated by divisive arguments on gender identity and the freedom of expression online. All too often, offline harms are amplified in online spaces, and different gender identities experience these harms in different ways.

Chair Ms Millar open the debate by asking: why are the Internet's safe spaces at risk? How can Internet governance better advance gender diversity and equality, and build an Internet that is safe, beneficial and secure and for all users?

Ms Akiwowo, founder of Glitch, a charity committed to ending online abuse, believes that the Internet can be safe. There are 'glitches' in the Internet that can be overcome by centring consideration of minorities in the design and governance of the Internet. Ms Akiwowo advocates for the introduction of transparency reports for technology companies, to better balance the power dynamic between companies and users. Ms Akiwowo drew attention to the lack of action taken by tech companies against white supremacy and the need to safeguard against harm.

Dr Hogan identified mutual antagonism as a cause of hostility, producing unsafe online spaces. Identifying authentic contributions to online debate can be difficult as often they are viewed with cynicism and understood to be insincere. For example, people with naïve or uncertain questions about a different culture or class could be categorised as hostile and associated with a certain group. Mr Hogan asked how we return to an Internet of joy where we appreciate others for being sincere?

Dr Hogan recognised that there is a lack of regulation globally on distributing generated images with a likeness to a person. This is leading to abuse. 95% of models on one of the largest platforms for generating images, Civitai, are of women. As it is difficult to identify if an image is fake or synthetic, generated images can be used to objectify and terrorise women causing significant harm.

Ms Moore opened with the benefits of the Internet for trans people, that is provides a space for people to connect, to help educate, organise and provide support for each other. Ms Moore outlined the harms faced by trans people, namely, doxing: collating information gathered about a person and publishing it, which can lead to trolling and hate crime. Ms Moore concluded that for Internet spaces to be safe without discrimination, its key that regulations don't assume the goodwill of government or platform owners and that the underlying technologies are architected to defend the rights of users by default.

It's only through a degree of ownership over our data, how we choose to associate and interact online, and being given the tools to defend ourselves from actors that aim to cause harm, that we were able to create the safe spaces that we need.

Ms Wilkinson recognised there has been an explosion in the diversity of gendered cyber harms and the gendered impact of cybercrime against a threat landscape, which is evolving too quickly and disruptively for policy, legislation, regulation and awareness to keep pace with. Ms Wilkinson recognised there are positive moves to adopt more gender sensitive approaches to anti-cybercrime measures, Internet governance and related fields such as ongoing conversations at the UN on gender mainstreaming across provisions on criminalisation. To support this work, Chatham House is developing a toolkit for policy makers and practitioners to integrate a gendered perspective in efforts to combat cybercrime. Ms Wilkinson concluded that a definition of Internet resilience should include meaningful connectivity, access and perception of safety online therefore if a diversity of gender identities can't access the Internet, this is a threat to its resilience.

DELIVERING DIGITAL TRANSFORMATION ACROSS THE UK

- Jacob Farrugia, Programme Manager, Digital Skills Council
- Harriet Perks, Learning and Development Lead, AND Digital
- Hollie Whittles, National Policy Skills Champion, Federation of Small Businesses

Chair Mr Faruggia opened the discussion with research which shows that many businesses and people across the UK are not equipped with the tools, skills, and digital infrastructure to take advantage of the digital opportunity and deliver growth. The panel discussed why this might be, including looking at the digital divide across different age groups and socio-economic backgrounds, as well as how leaders can ensure that we are able to make the most of technology and that everyone has the right skills to do so – keeping in mind the 9th Sustainable Development Goal set by the UN of investing in ICT access and quality education.

Ms Whittles outlined research from the Federation of Small business that 78% of small business across England are struggling to recruit due to the aging population, lack of digital skills, rural infrastructure, high recruitment agency feels, salary expectations and desire to work from home. Only 17% of small businesses are engaging with schools and education despite 48% of business owners recognising that digital skills are vital to the future growth of their business. Ms Whittles advocated for businesses working with education to bring subjects to life by articulating digital pathways to students, for example learning maths is a gateway to coding, machine learning and AI. Ms Whittles concluded that digital skills can remove the barrier of location for work and retain younger workforce in rural areas however this is reliant on strong infrastructure being in place, which is not yet consistently the case across the UK.

Ms Perks highlighted research from AND Digital that identified that the UK is losing 63 billion pounds per year in potential gross domestic product opportunities due to the digital skills gap. The research identified there is a misconception about what digital skills are, and 58% of respondents reported that they had never received digital upskilling at work. Additionally, leaders are often unaware of skills present in organisations and what skills are considered important. Ms Perks recognised the benefit of the introduction of the Department of Education's Essential Digital Skills Framework, however noted it had not been translating into schools. As careers are stretching to longer than five decades so we need to consider how to upskill and reskill the workforce to ensure we continually adapt and flex to the transformative shifts that are happening across the sociopolitical sphere. This can be achieved by having a deep understanding of what digital capabilities are needed, identifying the gaps, and creating the right environments and access to upskill and reskill appropriately.

MINISTERIAL ADDRESS

- Paul Scully MP, Minister for Tech and the Digital Economy, Department for Science, Innovation & Technology

The Minister opened his address by thanking the UK IGF for the invitation to contribute to and his anticipation for the upcoming UN IGF conference in Japan. He stated that whilst the Internet should be seen as a force for good, the associated challenges of using it, such as harmful content and disinformation, have meant that the government has progress its Online Safety Bill to ensure that the UK is the safest place in the world to be online. The Minister emphasised the importance of collective action to manage the Internet as a vital resource and raised the issue of Internet fragmentation as a serious threat. Stakeholder input from governments, businesses and technical experts is essential to develop effective policy, and he attributed the success of initiatives like the Online Safety Bill and the Data Protection and Digital Information Bill to such collaboration.

The Minister reaffirmed the UK's commitment to a 'free, open, and secure Internet with the day-to-day management led by the private sector and technical community', in the face of recent proposals by Russia for enhanced multilateral, rather than multistakeholder, governance of the Internet. The UK government believes that all stakeholders have a part to play in Internet governance and credited the IGF Network's ability to foster cross-stakeholder dialogue on critical global decisions related to the Internet. He highlighted the IGF's growth from its first session in Athens in 2006, to its current intercession work and over 150 regional, national and youth forums.

The Minister expressed optimism about building an Internet that benefits everyone, citing instances like the Internet's role during the COVID-19 pandemic and community network initiatives in Africa. While challenges remain, stakeholder collaboration is key to addressing them and bringing 'prosperity, security and opportunity to communities in every corner of the globe.'

UK INTERNET GOVERNANCE FORUM REPORT 2023

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 Science, Innovation, & Technology

CHATHAM HOUSE

GLOBAL PARTNERS DIGITAL

ORG OPEN RIGHTS GROUP