



UK Internet Governance Forum

UK IGF 2018 Submissions

Title	Topic description
Urgent need for trusting Domain Registration and Certificate Issuance	The Avalanche criminal network takedown involved more than 800k domains. Most of these involved fake companies and fake details, mostly involved in increasing criminal activity. Two more criminal networks have since been taken down, with similar results. A much stronger enrolment for company domain names is required. Possible solutions exist but are not being used because there is strong voice to fix the problem.
Machine learning and the impact on internet security	The algorithms that support machine language might be used to overcome security controls that organisations deploy to protect their businesses. I am not sure if this area has been sufficiently explored and thought of to formulate policies.
Preparing teachers for dealing with issues surrounding e-safety and cyber security	How can we best prepare our teachers for dealing with issues such as sexting, cyber security, radicalisation and other online threats to pupil wellbeing.
Keeping your identity safe online	Surveys have shown a rapid increase in online fraud. Misappropriation of identity stops some people from getting the benefits of online commerce. The UK aspires to be 'the safest place to do business online'. This needs discussion in a panel session.
Technology knows	
Personal, professional and organisational responsibility and liability for products, services and conduct in the on-line world	The current on-line world is based on a mix of 'best efforts', 'service level agreements' and complex contracts which mix draconian (but probably unenforceable) penalties on the part of customers/users with liability avoidance (e.g. innocent carrier, software as a service not a product) on the part of suppliers. Is that sustainable in the face of public disquiet with the behaviour of dominant suppliers and their acolytes. What is, or should be, the responsibility of technicians and professionals when faced with egregious behaviour? What should be expected of professional bodies faced by abusers with deep pockets and/or possible 'men of straw' those backed by 'no win no fee' lawyers? Is an IoT device subject to Product Liability law? Will good

	practice (as in medicine or aerospace) end up with a mix of renewable certificates to practice linked to mandatory insurance?
The convergence of virtual and physical systems and the new forms of governance the resulting hybrids will require	Offline retailers are beginning to seek to emulate the data exploitation practices of their online counterparts while online businesses are seeking to expand their data tracking into the physical world. In some cases, this takes the form of mergers (Amazon - Whole Foods); in others it takes the form of expansion via technology (Google - Android - Google Glass - DeepMind); in still others it takes the form of deploying data-gathering systems that join the physical world to the virtual one (Blip Systems, which deploys sensors in airports and railway stations). We need to begin thinking about how the last 25 years of laws designed for cyberspace will fit cyber-physical space.
Standards for online services provision	The extent to which internet-mediated and connected services now permeates society, and in particular the growth of online-only services, has not been accompanied by significant quality of provision. The usability, robustness and security of online services are currently dependent on the idiosyncrasies of individual web developers within a culture that has little or no appreciation of either human interaction or basic engineering principles. We need to consider how to bring this growing problem under control in order to ensure that online services are usable, reliable and safe for the public, for whom the availability of alternatives to them is diminishing rapidly.
Internet safety strategy / Tackling harmful content and behaviour/ AI standards and codes of practice/ Cybersecurity and IoT	Presenting and engaging stakeholders on the UK govt priorities.
GDPR redaction and the impact on online crime prevention	In many circles the threat of removal of publicly accessible WHOIS data has led to protest from law enforcement, IP rights groups and some governments. ICANN's position has not been at all clear. Given the timing of the UK IGF meeting, it would be interesting to review the experience of the first six months of GDPR, report on any emerging trends and practices, and discuss ways forward which balance legal requirements for privacy against transparency and safety/ security issues.