UK
Internet Governance Forum

Annual Meeting Report
28th November 2016

Zack Coleman
Valideus Ltd

Table of Contents

US Internet Governance

Lawrence Strickling, US Assistant Secretary of Commerce and Head of NTIA

Assistant Secretary Strickling presented the IANA stewardship transition as a tremendous success for the multistakeholder approach to internet governance. In a high level overview, it was explained that the expiry of the IANA functions contract represents the fulfilment of an almost two-decade old commitment by the US government, and one which cannot be reversed by the next administration.

Stickling suggested that this success – which saw the IANA functions contract expire on 1st October 2016 – is compounded when these events are understood in the context of the developing multistakeholder approach to internet governance and policymaking, an approach which the US strives to promote. Since the NTIA announced its intent to transition key internet domain name functions in March 2014, the multistakeholder community have collectively contributed over twenty-six thousand working hours, exchanged thirty-three thousand mailing list messages, and conducted over six hundred meetings in developing the transition proposal; Strickling thanked the community for these considerable, timely efforts, while also suggesting that there remained work to be done, particularly with regards to ensuring that the multistakeholder community hold ICANN accountable to the commitments it has made.

Strickling speculated that consensus decision-making, which characterises the multistakeholder approach, might be a viable mechanism for dealing with other policy challenges, citing data protection, software vulnerabilities, and artificial intelligence as examples. He opined on the strengths of the multistakeholder model, as being an effective decision-making process which: includes and integrates the diverse views of stakeholders, ensures underrepresented groups have a meaningful say in the policies that affect them; produces outcomes that are consensus based, reflects compromise, and are supported by the greatest number of stakeholders; builds agendas through bottom-up contributions rather than delivering top-down mandates; and earns legitimacy by practicing openness, transparency and developing an environment of trust. Dwelling briefly on legitimacy, Strickling posited that participants must trust those convening the multistakeholder process, and, gesturing towards the IETF, suggested that trust and legitimacy need not always be gained through government agencies underpinning any process.

However, Strickling also noted that the multistakeholder model has its limits. For one, it has not always been successful; the NetMundial Initiative, which followed in the wake of the successful NetMundial conference, was unsuccessful particularly because it was a top-down initiative which failed to solicit both the business community and the Internet Society. A second weakness of the multistakeholder model is that it cannot guarantee that all parties end satisfied; some aggrieved parties sought intervention from the US government as a remedy to issues arising from ICANN's new generic Top Level Domain programme. As partial remedies, Strickling suggested that those who believe in the multistakeholder approach must bring their concerns to bear within that process, and respect any outcome – this requires business leaders and policymakers have ample opportunity for participation, together with awareness of multistakeholder fora and their advantages over more traditional regulatory approaches.

Strickling concluded that with the success of the IANA transition, the challenge for the multistakeholder community is to build on that experience and find opportunities to apply the model to those issues where it has the best chance to succeed. He acknowledged that national and regional IGFs are integral to this process.

The Global Policy Landscape

Ed Vaizey MP, Former Minister for Culture, Communications and Creative Industries

Ed Vaizey MP contextualised the global policy landscape as having inevitably shifted with the completion of the IANA transition, an action which finally dispels the euphemistic perception that the internet was a creature of the US government, and instead demonstrates a concrete manifestation of the US government's commitment to a bottom-up multistakeholder model. Vaizey thanked Assistant Secretary Strickling for so adroitly managing the US government side of the IANA transition, before continuing to thank Malcolm Harbour (MEP) and Mark Carvell (DCMS) for their respective, continued efforts.

Referring to an article carrying his name in Tech Crunch, Vaizey restated his belief that the IGF is *the* governance forum of the internet, adding that despite knowing this was a controversial perspective, he firmly believes that the IGF is the primary fora for internet policy issues, in the same way that the IETF is the primary fora for technical issues. Vaizey suggested that in order for the IGF to continue to remain relevant, it must be adequately funded, well attended and vigilant against threats.

Questions and Comments from the Floor

Baroness Rennie Fritchie, Assistant Secretary Lawrence Strickling, and Ed Vaizey MP

Louise Bennett (BCS) articulated the view, garnered from the UN IGF, that African countries see EU privacy laws as a trade barrier and that this is represents an under-attended perspective. In response, Strickling noted that developing countries may yet need to develop particular stakeholder groups, particularly civil society, and that this might assist in breaking the singular voice on a policy judgement. Vaizey continued that every government has a view on these policy issues, even if somewhat benign, and that any scepticism might previously been justified.

Andrew Puddephatt (Global Partners Digital) spoke about the reception of NetMundial, noting the Russian and Indian government delegation's public dissatisfaction, by way of demonstrating that the multistakeholder model has only been endorsed by a small number of governments, and further, that the UN IGF mostly comprises civil society. Strickling clarified that while the NetMundial conference was well executed, his address reflected on the later NetMundial Initiative. Addressing the underlying question, Strickling compared voting figures between the December 2012 WCIT, where 89 countries voted to increase ITU engagement in internet issues, against the March 2016 GAC outcome, where approximately 30 other governments approved the IANA transition recommendation, as evidence that government support for the multistakeholder model was increasing. Vaizey noted that the countries in play are those undecided, and that any education and outreach effort should focus on these; Strickling agreed.

Ta-Wei Lin (Fulbright Scholar) highlighted the difficulty of education and inclusion in the digital reality of fake news, social media and the attention economy. Vaizey counselled that the IGF ought to be brought into the mainstream, with ambassadors attending other conferences and industry events, drawing attention to the work of the IGF.

Plenary One: Brexit, what next for UK Internet Policy?

Charlotte Holloway (TechUK), Jamie Bartlett (Demos), Malcolm Harbour (Former MEP), and Chris Francis (SAP)

(1a) Charlotte Holloway (Chair) offered a brief introduction of the panellists and setup the plenary by restating the agenda teaser. As Policy Director for European Exit at TechUK, she highlighted the challenge of separating digital value chains, before seeking the panellist's views on the fault lines of post-Brexit internet policy.

(1b) Jamie Bartlett articulated his overwhelming concern that the internet is becoming more difficult to govern, not least since many individuals actively seek ways to avoid regulation. Gesturing towards his recent publication, 'The Dark Net', he noted the increasing trend of stolen personal information, and the apparent ease with which companies avoid website takedown. Bartlett continued that people have been preparing themselves for world leaders who don't respect privacy – for example by using freely available encryption – and that President-elect Trump might be the person privacy activists have been warning people about.

(1c) Malcolm Harbour followed, with the preamble that Brexit is the result of people not trusting European decision-making, and indeed MEPs. He noted that every piece of UK legislation relating to the internet has been developed in conjunction with the European Parliament, since the UK was part of the EU before the internet became ubiquitous, and that the House of Commons is not designed to deal with detailed legislation. He welcomed the decision to implement new European data protection regulation, as it permits the continued free exchange of information.

(1d) Chris Francis observed that trade flows have already changed as a result of the internet, but that this demands: (a) legal compliance, usually including (b) a trade agreement, and (c) data governance. He advocated for consistent regulatory approaches, which allows business-to-business operations to work fluidly.

(2a) Holloway refocused the discussion on the challenge to policymakers. Noting that on top of disruptive technologies like IoT and AI, the Great Repeal Bill will require 2000-3000 statutory instruments, she offered panellists an opportunity to comment on the way core regulatory issues are addressed in parallel with Brexit.

(2b) In response, Bartlett speculated that the UK has never been able to stay ahead of regulatory issues, not least since regulation only takes account of current business practices. As a partial remedy, he suggested legislation ought to satisfactorily resolve some hypothetical scenarios, including a bedroom start up selling into a non-EU country; and company purely on a blockchain, paid for using cryptocurrency and organised using smart contracts – either of which might be the future model company.

(2c) Harbour focused on the need for better international cooperation, emphasising the challenge this represents given that Europe, a bloc of friendly countries, have failed to reach substantive agreement on politically salient issues such as taxing corporate revenue. Harbour offered the takeaway that even though we might seek to be outside the European Union, we cannot absent ourselves from the global political process, reiterating his support for UK adoption of EDPR and the tougher environment it creates.

(2d) Francis again suggested that notwithstanding disruptive technologies – be that IoT, Industry 4.0, future factories, or appification – any solution must work in a coordinated framework. He continued that the political debate ought to re-centre on workable solutions, drawing attention to the number of open portfolios that include aspects of the digital market, by way of suggesting these efforts should not be siloed.

(2e) Harbour followed up, in response to a brief mention of EDPR, that Prime Minister May has a history of successfully exercising a universal opt-out, and subsequently, piecemeal, opting in – as exemplified by her approach to EU regulation on security and justice. Harbour estimated there to be 12,800 pieces of European legislation, and that over a 5-6 year period, the UK would have to decide which ones to opt-in to.

(3a) In the first question from the floor, Tim Barnes (Nominet stakeholder committee member) sought the panel's views on alternative approaches to supranational negotiations on technology policy. Harbour suggested technology policy should be the result of multistakeholder interaction, and that EU decision-making was actually more transparent than many national governments. Bartlett hinted that supranational negotiation was unavoidable, while Francis spoke to the potential leadership opportunities for business, for instance by demonstrating open data policies in the way Transport for London have.

(3b) The second question, from Sabine McNeill (TechUK member), drew attention to the governance-government frame, as a preamble to soliciting the panel's thoughts on possible accountability mechanisms suitable for Brexit decision-making. Francis drew attention to the 'better regulation' policy practice, where a consultation necessarily takes three months – so that, for instance, large representative organisations can coordinate a response – balancing this against the time constraint involved in Brexit negotiations. As an alternative, Francis highlighted the Government Digital Service strategy, whereby consultation comments are submitted online, and made publically available, such that people and organisations – including government departments – can respond inline to other submissions. Harbour referenced the IANA transition, and the utility of policy interfaces such as mailing lists. Bartlett advocated for broadening the demographic involved, for instance by including the intelligent individuals operating in the quasi-criminal space, or appreciating that millennials might have different, but no less important, notions of how to arrange the internet.

(3c) Louise Bennett (BCS) engaged the panel on the topic of EuroDIG, seeking their perspectives on its sufficiency for ensuring multistakeholder governance. Harbour clarified that EuroDIG is a dialogue process not a governance process, and instead offered the Council of Europe as a body active in suggesting international governance frameworks; noting that Brexit does not necessarily affect Britain's Council of Europe ties, Harbour proposed that Britain apportion it more significance. Francis considered the tension between a bottom-up political process, characterised by what works, and a top-down process, characterised by IGO politics. Next, he drew attention to the two hundred global facing standards consortia – that have the backing of those tasked with implementing standards – by way of suggesting there remains the possibility of success in-between these two conceptual processes. He closed out the questions, by suggesting governance debates should not be highly legalistic or academic – as perhaps debates surrounding regulation of privacy and data have become – but should retain specificity insofar as they speak to problems in, for instance, a particular sector.

(4) Holloway concluded the session with a brief summary of its contents, thanking the panel and audience for their time.

Plenary Two: What is the Impact of the Internet on Political Debate?

Seb Payne (FT), Toni Cowan-Brown (NationBuilder), Carl Miller (Demos), and Dan Hodges (Mail on Sunday)

(1) Seb Payne (Chair) opened with the statement that the last five years have seen an increasing number of populist uprisings played out, in part, on social media – citing the Arab Spring, Brexit referendum, and Trump election as examples. Turning to the panel, he invited them to characterise the relationship between the internet and politics, as either encouraging or dis-incentivising participation.

(2a) Toni Cowan-Brown began that the internet encourages political participation. Drawing on NationBuilder – introduced as a tool which equips both community leaders and Presidential candidates alike – she suggested there is now a greater range of funding models available, as popularised by President Obama's 2008 campaign. Cowan-Brown continued that Jeremy Corbyn's raising of £250,000 in £2-£5 donations engaged new people in politics, especially by securing repeat donations, an approach made possible by a clear funding model. Finally, she indicated campaigning was not all about big data, to the extent that *N* email addresses, without any information about those individuals, was just a mailing list.

(2b) Dan Hodges countered the view that the internet had any clear impact on politics. He began with the suggestion that a year ago, he would have said social media was a disaster, mostly for the left, as characterised by Ed Miliband supporters speaking to themselves in an echo chamber. However, post-referendum, where social media was significant in both the winning and losing strategies, Hodges challenged that there was any evidence that social media has an actual impact on politics. He continued that the swing Brexit demographic were people new to voting – as evidenced by their needing to ask about the voting procedure – probably not those same individuals retweeting Nigel Farage. On money, he noted that Hillary Clinton outspent President-elect Trump by 2:1.

(2c) Carl Miller responded that the internet is encouraging participation, particular for a younger demographic. Against a backdrop of declining trust in politicians, party membership, and youth turnout, Miller noted 'The Rise of Digital Politics' paper, which found that 50% of respondents used social media, 70% of those answered that they felt closer to politics as a result, while 40% responded that they would be more likely to vote as a result. Addressing Hodges' call for empirical evidence, Miller noted that there can be no deterministic link between social media and campaign outcomes, as this would require an impossible number of controls; nevertheless, there are a number of studies confirming the presence of echo chambers, which have been found to cause polarisation and the belief that those outside a particular echo chamber are either ignorant or evil. Miller suggested that the social media frenzy was too orientated around elections, rather than daily political activity.

(2d) Hodges countered Miller's evidence, in particular that if young people followed through on their being 40% more likely to vote, then given their voting trends, the results would have delivered President-elect Clinton and Prime Minister Miliband. On the topic of traditional campaigning being redundant, Cowan-Brown expressed the belief that that tools like NationBuilder are not about replacing old with new, but that the way forward should be integration.

(3a) Payne introduced a second topic, the role of news outlets, noting that fake news got eight times the prominence of factual stories in the US election. In response, Miller offered the suggestion that the Facebook news editor is the most powerful editor in the world, and yet it operates without scrutiny or the possibility of redress; more particularly, that Facebook are the only people who can comment on the fake news story is concerning. Next, he speculated that the professional journalist is on the way out, in favour of new voices who have no sense of journalistic ethics, balance or fact-checking. Tying the two previous points together, Miller opined that the age where we can control information entering into public life is over, since it is much easier to upload content than remove it. He proposed digital literacy as a solution, to a problem that is becoming urgent for democracy.

(3b) Hodges offered the history behind Facebook's choice to remove human editors, as a result of a challenge from the US right. Hodges proposed a solution of simply trusting the electorate – if an individual has read the majority of an article of Hillary Clinton's use of black magic, they are unlikely Hillary voters. On a different tack, Hodges noted that the news stories dominating the US campaign were undisputed – for instance Clinton's use of personal email, or Trump's comments on women – perhaps an indication that the electorate has been desensitised to sensationalist media.

(3c) Miller and Hodges debated the evidence base for campaign interventions, with Miller arguing that cause-effect evidence is impossible, and that individuals are notorious at assigning levels of influence; Hodges countering that any revolutionary calls regarding the impact of social media should be evidence led.

(4a) Payne introduced the third topic, the necessity for, and instruments of any government intervention surrounding the internet. Cowan-Brown suggested legislation would always be required: for instance, a driverless car requires roads funded by taxpayers. She continued to draw a distinction between social media and the internet, suggesting that it is not possible to legislate the internet, only its constituent parts.

(4b) Miller strongly rebutted any claim that the government should regulate content online, but distinguished this as separate from the regulation of campaign activities: for instance, regulating the output of campaigns – such as the £350 million per week saving statistic quoted by the leave campaign – or the spending rules for online campaigning. He continued that much of the activity on social media surrounding campaigns was not in fact orchestrated by those campaigns, and as such, implementing and subsequently enforcing any rules would be exceptionally difficult. Cowen-Brown added that regulating data is another way forward.

(5a) In response to two remote interventions, the panel were not optimistic toward the possibility of regulating the internet at the global level, since there are no global political structures. Later, Miller proposed a 'Royal College of Algorithmicians' as a method for ensuring professional algorithmic standards.

(5b) The first question from the floor focused on digital engagement and young people. Cowan-Brown suggested that the voting age in the UK was best understood as a proxy for having sufficient education and sense of citizenship. Miller highlighted the successes of the Digital Democracy Commission, in securing online voting for MPs, and expressed a wish that this would catalyse a slow, safe, but nevertheless innovate approach to digital engagement in democratic politics. Hodges expressed the cynical view that parties who wished to change the voting age were simply those that would benefit, and that this decision was driven by a desire to win rather than any sense of principle.

(5c) A comment from the floor, by a commissioner serving on the Digital Democracy Commission, addressed Miller's statement, framing electronic voting as arising out of a desire to making voting records more transparent for the electorate. Miller indicated that more information just engages the already engaged, and that an alternative way forward would be to nudge a digital element into local level decision making.

(6) Payne thanked the panel and audience for their contributions.

Sponsors Address

Russell Haworth (Nominet)

Russell welcomed the participants back to the afternoon's proceedings. He outlined how some of the complex technical and institutional scaffolding behind the scenes is not always immediately obvious but the internet architecture and internet governance structures are inextricably linked and sometimes diametrically opposed but are always critical to our vibrant digital future. The internet forms over 10% of the UK's GDP it is critical that we have a good forum for discussions on the impact of the internet on society.

Nominet is the country code manage for .uk with over 10.6 million domain names under management. Concerned with keeping the UK's internet reliable, free from crime as much as possible and make it a safe place for people to interact and transact.

Russell highlighted how he believes the UK IGF is reaching a new level of maturity and that many of the topics on the agenda today will feature in discussions in Mexico next month at the IGF.

Russell closed by thanking the UK Government for their continued support of the UK-IGF and introduced Rt Hon Matt Hancock, Minster for Digital and Culture.

Keynote Address

Rt Hon Matt Hancock MP, Minister for Digital and Culture

Source: https://www.gov.uk/government/speeches/the-future-of-the-internet-freedom-in-a-framework

It's a great pleasure to be at the UK Internet Governance Forum – my first as Digital Minister – and a crucial event in the life of the Internet's governance.

It's a great honour to speak here because I feel my life, like so many of yours, has been bound up with the development of the net.

I still remember my first online communication, to a friend who lived about a mile away, when a dial-up literally meant dialling his number. The phone bill wasn't pretty.

I remember being astonished by how he got a new number so he could dial up something called an Internet Service Provider, and that the number of minutes he spent on the phone line didn't affect his bill. It was amazing. I wonder what ever happened to those Internet Service Providers. Anyway, the best thing was the rest of his family were delighted as the new line meant they could start making phone calls again.

I remember like yesterday Clive James's series on TV called the "information super highway" where he devoted a whole series to laughing about the idea that - sometime in the future - we could write to each other and reply immediately over a phone line, or find information from a library on the other side of the world. Amazing. I hope someone followed up on that.

And then I remember the time Steve Jobs said that the entire history of the world – more information, better organised, and more freely available than ever before – was about to become available in everyone's phone. I thought they'd really nailed data compression. Wrong. They'd invented the smartphone.

Now of course the Internet is a central part of the lives of most people on the planet – at the core of human relationships, business, education, trade, entertainment: humanity is connected like never before and the impact is everywhere.

Small wonder, then, that I'm excited to be here at the Internet Governance Forum. It matters to me, it matters to you, and it matters to most people on the planet.

Our connected world underpins our prosperity too, with millions of jobs and billions of value directly linked to the Internet. Connectivity is no luxury but a must – and I've got a whole other speech on broadband if you want to hear it.

But today I want to share with you my thoughts, born of my experiences in tech both as a citizen, in business, and as a Minister.

I want to address governance very directly, because I believe that governance matters.

But before I do that, I want to address how I believe we should think about the way the Internet is run.

There is an argument, which has deep roots, that the Internet is both ungovernable, and oughtn't be governed.

I want to discuss this argument very directly.

My starting point is that the Internet is a great force for freedom. It is an invention of humanity, for all humanity, and radically democratising, liberating, and enervating in its operation. The Internet transcends borders and brings people together like never before.

This is a huge and progressive change.

Yet it brings with it challenges, as it disrupts established ways of doing things. As a tiny example, remember the crises of email rage a decade ago, as people learned how to write, and respond to emails, in a way that needed to be different to their approach to phone calls or letters.

Email was progress, but that progress needed cultural change to harness its power for the good, and stop the progress – email – leading to reversion to animalistic behaviour as email rage unintentionally stoked tensions.

Twitter democratises people's voices, but has increased online abuse too. I'm pleased to see the policy changes they announced earlier this week around hateful conduct and muting functions.

Tinder, Uber, Amazon: they all improve people's lives overall but need careful handling.

And the thing about these sorts of trade-offs is that they are not new.

Finding a way to organise ourselves, without higher authority, to maximise the opportunities and mitigate the costs is no new challenge.

In fact, it's been around for as long as man has lived in communities.

We don't have to invent a theory from new, but can draw on political philosophy. The context is new. The technology is new, the scale is new, and practicalities different. But the principles aren't. The principles go back to Athens.

I think the way we address it can be summed up as follows:

The Internet should be free, not lawless.

Open not laissez-faire.

Liberal, not libertarian.

Freedom is a framework.

Burke said that liberty "is not solitary, unconnected, individual, selfish liberty, as if every man was to regulate the whole of his conduct by his own will". Instead he said liberty is "social freedom". "Secured by the equality of restraint." In which "no one man, and no body of men, and no number of men, can find means to trespass on the liberty of any person."

Taking that fine principle and applying it to today's problem means protecting liberty on the internet with reliable protections against theft, and harassment, and child pornography, and incitement and terrorism.

The Internet is a phenomenally powerful agent of commercial and social progress. That is to be applauded and cherished. But it is also a medium for fraudsters, thieves, extremists, terrorists, and those who want to hurt children.

That's not new. The world – online and off – is an agent of commercial and social progress. But it is a medium for fraudsters, thieves, extremists, terrorists, and those who want to hurt children too.

Put it this way: we highly value freedom on the Internet. We want the Internet to be free, open and global. We reject the vision of a censored and limited Internet, controlled by national governments.

And we are also clear that this free, open Internet is not a licence to abuse freedom, to cause harm. In the off-line world, we have longstanding boundaries on free speech, to stop people using it to incite racial hatred or violence, for example, or libelling others without consequence.

I want to make an important point today about self-confidence in our values. The fact that we as a society have put these boundaries on acceptable free speech has not undermined our status or credibility as a society that values free speech. No-one can credibly say that because we stop people standing up and spreading racial hatred means that we are on the side of repressive regimes and not free speech.

We have been mature enough to accept this in off-line speech. As the Internet matures so we need to accept these principles online too.

A free and open Internet does not mean an Internet without boundaries or rules. And agreeing as society what those rules should be does not weaken our commitment to freedom.

As Tim Berners-Lee has argued, let us have an approach of open standards within a commonly agreed rules-based framework.

My vision – our high goal – is of an Internet that is a catalyst for creativity not for harm, based on these principles of a rules based framework.

We believe in an Internet open, trusted, and secure that serves freedom and the economic and social development freedom brings, and protects human rights of privacy, access to knowledge, and freedom of expression - open to debate and challenge, with no political ownership where the logic of an argument can be tested and found wanting.

We want Britain to play her part in leading that debate.

So how do we make that happen in practice?

By its nature: global and fast-moving, legislation that is national and slow-moving will never be the perfect tool for Internet governance.

So industry and the public have important roles.

Social networking sites such as Facebook, Twitter, YouTube and others all have abuse-reporting services.

UK ISPs act on notifications of potentially illegal content – and this self-regulation is incredibly important.

Members of the public are now able to report online material that promotes terrorism or extremism to the Counter Terrorism Internet Referral Unit, via GOV.UK.

All sensible businesses take steps to protect themselves from cyber-crime.

Our new, non-statutory National Cyber Security Centre ensures that government plays its part.

Search engines, platforms and ISPs play their part in removing harmful material. Later this afternoon, my colleague Joanna Shields will tell you what we are doing to promote child Internet safety at home and abroad. We are having success with partnerships in tackling some of the toughest challenges in this area.

It is vitally important that all those who cherish our free Internet play their part in taking responsibility to address these issues.

In short, we need to develop a set of norms that guide appropriate behaviour towards the Internet in free societies.

A wide gap has opened up between our adoption of technology and our ability to create frameworks and norms for that technology.

The governance of the Internet is just one area where practice has run way ahead of society's ability to think through the consequences and set rules to ensure the impact of the technology is most positive and least harmful.

There are many others, from the fact that our children do most of their socialising online, to the growing realisation that the market is often a poor judge of the true value of technology, unable to capture massive externalities both positive and negative.

If we do not find a way to build norms for new technology, starting with retrofitting it to the technology that has already become pervasive, then the gap will continue to grow.

And when this gap grows, it's harder to bring the public with us.

More substantively, some of the technology does actually need to be regulated - it will more beneficial and less harmful when it is operating in a thought-out framework.

But the speed of innovation is now much faster than the speed at which society can create norms.

And given the innovation is global, we cannot slow its pace and must therefore gear ourselves up to handle the pace.

So norms are important. But this non-statutory action alone is not enough.

The Internet should be characterised by freedom, not lawlessness.

The legislative framework matters.

Our starting point is that the law of the land applies equally, offline and online: what matters is the substance, not the medium.

So we are for example equalising our copyright laws in the UK so they are equivalent on and off line. Laws to protect intellectual property are just as important on and off line, as intellectual property is still property, no matter how it's propagated.

And in other areas too, like in requiring age verification of adult materials to protect children, we are legislating.

But in many others, like removing terrorist or child abuse material, we operate on the basis of non-statutory co-operation.

And that brings me to global Internet governance.

No one international institutional has oversight or control of the Internet. We have instead a decentralised system, where international Internet matters are addressed by a variety of organisations, including the United Nations and its Commission on Science and Technology for development and UNESCO, and the Council of Europe, addressing the importance of freedom of expression, cybercrime, privacy, and human rights.

We have to ensure that governments, civil society, business, the technical community, academics, and Internet users all have a voice in these global Internet governance mechanisms. That is the only way to make them inclusive, transparent, accountable, and fit to serve the best interests of the Internet using public around the world.

Following ten years of dramatic Internet expansion, the UN General Assembly last December recognised the value of a multi-stakeholder model of governance.

The General Assembly endorsed the success of the Internet Governance Forum – the global IGF. This was important.

The IGF is the key meeting point of Internet standards-making bodies, and does a very good job, championing the merits of participation and reporting multi-stakeholder work directly to the UN Secretary General.

The fact that the UK Government – along with many others: other governments, Nominet, civil society organisations, and business – contributes financially to the IGF is a testament to the value of its work.

The key question is not whether there are boundaries, but how those boundaries are made. If they are made by governments unaccountable to their own people, and nationally, then the boundaries will have much less legitimacy than if they are clearly made by society thinking and acting together. And if they can be agreed internationally, then it has still more legitimacy.

This is the logic of the model of multi-stakeholder governance.

The name was clearly designed by a committee, and doesn't make the heart sing. But the underlying concept should. Because what it says is this - we do not entrust the rules of the Internet to any one country or part of society. Rather, because we value its freedom and openness so much, we entrust it only to a parliament of society, in which we all have a voice.

Yet the IGF cannot stand still. It needs to move forward with a greater focus on what it can contribute to sustainable economic growth and increased social wellbeing.

At a national and regional level, multi-stakeholder events like this one today – and those in other countries that have replicated the UK model – are extremely useful for the sharing of best practice and ideas for technical solutions and policy responses.

I am especially interested in ideas for strengthening the resilience and security of local networks and in practical solutions for setting up Internet exchange points, which can have a significant impact on reducing costs and stimulating local content.

And on the question of IP addresses – the index of the net – now that the US government has stepped away from its sole oversight role, and the transition to a global multi-stakeholder group is now underway – the rigorous scrutiny of the system must endure.

The current raft of reviews into accountability, transparency, diversity, and inclusivity are absolutely necessary - because the digital economy simply cannot work without an efficient, fully functioning domain name system.

I know some of you here are actively involved, and I am grateful for what you are doing.

The global nature of the system is reflected in the 170-strong membership of the Governmental Advisory Committee. That breadth needs to be fully integrated with all levels of policy development and oversight, because that is the framework that has been proven to deliver a secure and resilient system.

This framework, in global governance, national rules, civil society, norms of behaviour and social responsibility, is critical to protecting the freedom of the Internet.

Freedom is not automatic, but fragile, and not just wished for but supported.

So let us pledge anew to the task of ensuring that this great innovator, this bringer of change, this invention that is changing the world and all of us in it, let us pledge again to work to ensure its freedom, that we may build on the opportunities it presents, for all mankind.

-- ENDS --

Plenary Three: e-Identification, the Future of Privacy?

Greg Francis (Access Partnership), Ben Cade (Trustonic), Sarah Munro (Barclays), and Robin Wilton (ISOC). Organised by Access Partnership

(1a) Greg Francis (chair) set the tone of the session by suggesting that for the internet is to continue to work, we must be able to trust our online interactions. With passing reference to examples of failure – the TalkTalk data breach, Tesco Bank hack, and Facebook fake news – he turned to the panel for their opening remarks.

(1b) Robin Wilton began that ISOC have framed their recent work in terms of trust and access, before offering a definition of trust as a belief that someone will act in your interest, even if they have the means and motive to do otherwise. He continued to suggest that technology can only offer a partial solution, since the roots of trust are analogue. Comparing trust and privacy, Wilton suggested individuals misrepresent trust online: using a separate bank card for online transactions is good in privacy terms, insofar as an individual mitigates risk, but less good in trust terms, since the vendor sees a lower income, less trustworthy customer, while the bank may not offer as favourable terms and conditions in the event of a misfortune.

(1c) Ben Cade explained that Trustonic embeds security into devices, and drew attention to the conflict between a company, who want to strongly authenticate the user, and an individual, who wants to share the minimum amount of personal information to gain access to a service. Cade compared different approaches to authentication: two-factor authentication, comprising something known and something owned, gives a terrible user experience; while single sign on is equally subject to vulnerabilities at an application level. He advocated for privacy to be dealt with at a hardware level, hence personal information has no reason to be stored remotely, and evidenced the South Korean approach of instituting every citizen a digital identity as one way in which governments can play their role.

(2a) In response to a question about current e-identification standards, Wilton gestured toward Security Assertion Markup Language (SAML), which has been in use for over a decade. Next, he complicated Cade's explanation by introducing federated identification – cases where a service provider relies on the assertion of your identity, but where an identity provider has offered that assertion. Reverting to standards, he caricatured the roles of the W3C, IETF and ITU.

(2b) Cade followed up by suggesting that the simplest route to mass adoption ought to be the overarching theme, and that having a standard was not necessarily the correct starting point. In this regard, he noted that individuals were increasingly comfortable with biometrics as a method of authentication, and that this solution is possible to scale.

(2c) Wilton, while agreeing with Cade, went on to challenge the framing of hardware solutions as flawless; the Snowden revelations made public the reality that governments had regularly been subverting hardware vulnerabilities. Wilton spoke of the IETF response, characterising the content of the revelations as an attack on the integrity of the internet, and the subsequent decision to begin an open source project to restore integrity into the supply chain of cryptographic products.

(3a) Francis refocused the discussion on regulation. Wilton advised that the route to critical mass is by convenience, and regulation is not the most effective way forward, since the overwhelming force is economic – service providers offer what they can monetise most conveniently. The place of regulation would be to modify the way the market is functioning, to incentivise privacy, although this is not the preferred policy option.

(3b) Wade echoed Wilton, insofar as he agreed that regulation should be the last course of action, but that for now, companies such as his own were allocating significant resources into ensuring that the market gets moving, that device makers know they are purchasing quality product, and that customers trust those authentication solutions. Wade suggested that although he represented the *de facto* market leader, he did not intent to secure monopolisation.

(3c) Wilton clarified that regulation should only be used to correct a foreseeable market failure. He offered the European Electronic Signature Directive as an example of top-down regulation: the Directive has been in place for years, intended as an enabler of e-commerce, but has had low uptake because individuals presumably determined that the threshold of authentication was unnecessarily high or burdensome. The more successful solution was more straightforward an audit trail, via a signed intermediary. This failure notwithstanding, Wilton noted that it remains right that government attempt to increase the appetite for trust.

(4) In advance of questions, Francis offered the panellists an opportunity for intermediate conclusions. Cade offered three points: that biometric authentication data ought to rest on the device, that strong authentication was key, and that more thought is required on how to collect and utilise such data. Wilton offered an acid test: that any identity scheme that cannot cater for pseudonymous or anonymous interactions, as determined by the user, should be considered deficient. Put another way, it should be possible to utilise trustworthy attributes of identity.

(5) In a question from the floor, Julie Dawson (Yoti) questioned the role of knowledge-based authentication when so much personal information is available online. Cade used his response to separate out the requirements an individual must fulfil to register for a service, against those required to authenticate identity. Wilton agreed with Dawson that knowledge-based questions were of limited use, since they are a shared secret, an oxymoron. Further, he noted that the majority of companies do not take the same care securing the responses to knowledge questions as passwords, despite these being equally significant.

(6) By way of conclusion, Francis solicited both panellists' views on the most important factor driving trust. Wilton responded that trust must be recognised as a social construct, and as such, must be understood as depending on more than technology. Cade seconded this, adding that trust conceptually requires security, and that the market must readily desire both.

Is the UK Prepared for the Threat of a Cyber Attack?

Professor Anthony Finkelstein (UK Chief Scientific Advisor for National Security), and Alistair Bunkall (Sky)

(1) Alistair Bunkall opened by offering a set of Professor Finkelstein's credentials, and started the interview proper by asking Finkelstein to explain his role. Finkelstein responded that his role comprised three parts: operating research and science programs across government, providing critical challenge within government, and participating in a network of scientific advisors on cross-cutting policies.

(2) Finkelstein noted the major themes of his role are located in the Strategic Defence and Security Review: countering terrorism, securing strategy advantage for the UK, and ensuring the state is collectively safe to operate in the cyber domain.

(3) Bunkall referenced the potential impact of cyber-attacks on the US election, after which Finkelstein spoke to the increasing realisation that democratic processes are, in some sense, part of critical national infrastructure, and thus should be factored into our protection strategy. Further, he advocated for a cross-departmental, coordinated approach to defend against cyber and other methods by which foreign powers seek to exert influence over the UK.

(4) Bunkall pivoted, to talk about recent Freedom of Information request made by Sky, which revealed that many NHS institutions had negligible or no spend on cyber security. Finkelstein, a board member on an NHS trust, stated that this represented a failure of governance responsibility by those NHS boards, who ought to be held to account. Finkelstein added that this also indicated skills are low, and understanding inadequate, at a strategy level where decisions are made.

(5) Finkelstein offered commentary on the framing of cyber security, that perhaps the narrative of the 'sky falling in' was somewhat premature, and that the National Cyber Security Centre was well positioned to provide advice and assessment. Bunkall posited that cyber security has been considered covert for too long, to which Finkelstein suggested that in general, situational calculations on a per case basis continue to determine when disclosures are made, or knowledge is retained. Finkelstein acknowledged that these decisions are an increasing subject of importance, and welcomed increased government expenditure on cyber security organisations and research, while also calling on private industry to get more involved in promoting mutually beneficial, structural arrangements.

(6) Bunkall proposed a triangle of involved parties: the intelligence agencies, private companies, and end users, and wondered if these are married together tightly enough. Finkelstein reiterated that the notion of critical infrastructure has been too narrowly drawn, and securing a wider range of critical infrastructure might have some effect on the triangle; he mentioned that each point on the triangle would require unique advice, and that this could be found, for example, at the National Cyber Security Centre.

(7) Finkelstein suggested that no security professional ever expects total security; rather, security should be conceptualised as an economic issue, where the goal is to ratchet up the cost of a potential attack, such that the cost would outweigh the benefits. Further, he categorised his perspective as that of a security optimist, described as the case where society faces rising software system vulnerabilities, but he retains the belief that we nevertheless have the makings, technology wise, to remedy these flaws – for instance, by improving development practice, or utilising formal verification or big data and machine learning.

(8) The first question from the floor related to the role of small businesses. Finkelstein advised that the whole marketplace should have access to the skills to secure their property, and the role of small business was to simply adopt the technology at market pace. He noted that a cyber-attack was more likely to utilise many shared surface areas.

(9) The second question regarded the effectiveness of market forces, citing TalkTalk's falling share price in the wake of their security leaks as evidence. Finkelstein suggested that this might not have sufficient weight, although continued that this was also not an argument for fines or stricter regulation.

(10) The third question addressed the role of the insurance industry. To this, Finkelstein explained that security is non-compositional property, meaning that two interconnected systems might be proven independently secure, but are nevertheless insecure when operating in combination. Since the properties of mixed systems are complex, he suggested that it would be difficult to predict the probability distribution of failure, and therefore the insurance industry might not be the correct location for a set of industry-raising standards.

(11) The fourth question attempted to clarify Finkelstein's title, particularly the word 'scientific'. Finkelstein noted that increasingly the government is more aware about the importance of evidence-based policy informing operations, and that the UK has leading expertise amongst governments. He added that national security professionals have a penchant for evidence.

(12) To close, Bunkall asked Finkelstein directly if the UK was prepared for a cyber-attack. Broadly, the answer was yes, to the extent that the UK pays a great deal of attention to this risk, has significantly invested in both long and shorter term strategies, exercises its capability regularly, and is a world leader in this regard.

Keynote Address

Baroness Shields, Parliamentary Undersecretary of State for Internet Safety

Source: https://www.gov.uk/government/speeches/an-internet-for-children-and-young-people

Thank you for inviting me to speak today. The Internet Governance Forum is a unique venue that brings together a wide range of stakeholders from industry, civil society, government, parliamentarians to academics. So it's a real pleasure for me to talk about a subject matter that I care very deeply about - children and young people.

I know everyone in this room thinks about the internet and its future. You ask: How can technology help us? How can businesses thrive in the digital economy? How can we stay safe from cyber-attacks? How do we keep the internet open and free for it to thrive? How does social media influence political debate? How can we reach the next billion internet users?

My colleague Matt Hancock spoke earlier about some of these issues. And I know these topics, and many more, will be debated by speakers and participants today.

Children and Young People online

As Minister for Internet Safety and Security, one of the things I think a lot about is children and young people. According to Ofcom 87% of children aged 5-15 go online. We know that the internet has been a game changer for them - as for adults - and that it has brought incredible opportunities. It can enrich the lives of children and young people by offering new ways to communicate and be creative, stay in touch with peers and learn about the world. With so much information at the tip of their fingers, they can research their homework, find peer groups online and seek support and advice if they need it.

When you look at the data available that you realize how the online world is a massive part of their lives. Last year Ofcom compared children's media access and consumption across ten years – between 2005 and 2015. It showed that:

- The amount of time 8-11s and 12-15s spend online has more than doubled. In a typical week, 8-11 year olds spend 11 hours online, up from 4 hours. For 12-15 year olds, it's nearly 19 hours. Up from 8 hours a week.
- There is less research on 3-4 year olds, but we know that over half of children this age use a tablet. And that over 60% of 5-15s also use one.

Since 2005, interestingly - but perhaps unsurprisingly - the mobile phone has overtaken the TV set as the device 12-15s would miss the most. And for the first time, those in this age group who watch both TV and YouTube, say they prefer to watch YouTube content to TV programmes.

Of children who go online, nearly a quarter aged 8-11 and three-quarters aged 12-15 have a social media profile. Just yesterday Ofcom reported that:

- For the first time 5-15s spend more time online that watching TV. That's 15 hours of time spent online. 87% of 12-15s use YouTube website or app.
- Take up of a social media account increases sharply between 12 and 13, from 50% to 75%.

So we know that young people spend quite a bit of time on the internet. Even prefer it to TV. Devices and online content start to become a part of their lives very early on. Many will also be sophisticated users of apps, and use a range of devices proficiently, including games consoles. This generation of under 18s will have different expectations from digital communications compared to adults.

While the internet has brought a lot of good, unfortunately, it also has its challenges. It reflects the ills and dangers in society. Children and young people in particular are vulnerable to a range of risks. They may be exposed to age-inappropriate material online such as pornography, violence or hate speech. They can fall prey to bullying. Their personal images could be shared online without their permission or they may seek to imitate dangerous behaviour. Under 18s may also not fully know how to protect their privacy and share where they live, or start to interact with strangers that can lead to threats and abuse, or in the worst cases, to physical, sexual or psychological harm.

Government's approach to child internet safety

I passionately believe that in order to protect children from harm and violence in the 21st century, we must act to secure their safety online. I'd like to share how the Government is doing this while ensuring children and young people continue to benefit from the opportunities brought by the internet.

The UK has in place a range of robust offences to protect children from sexual abuse, exploitation and exposure to harmful material and activity online and offline. We are also passing new legislation to ensure that children are restricted from seeing commercial pornographic content online. While Government itself can drive change to improve child internet safety - and will continue to do so - our frame of mind is similar to supporters of the UK and Global UN IGF: we believe in the benefits of multi-stakeholder efforts and in building long-term partnerships with industry and other experts.

Multi-stakeholder approaches are hard work. It requires a common understanding of what's important, a vision for the future, and a drive and commitment by a range of people and organisations that may not be a natural fit. I have been privileged to work on two initiatives with such a strong purpose: the UK Council for Child Internet Safety and WeProtect. And my conclusion is that the whole is greater than the sum of the parts.

The Government is committed to improving the safety of children online and have a strong track-record in working with the internet industries and the charity sector to drive progress. At home, we have the UK Council for Child Internet Safety (UKCCIS), a multi-stakeholder forum representing over 200 organisations with an interest in child internet safety. I am one of its co-Chairs, along with Ministerial colleagues from Education and the Home Office. The UKCCIS Executive Board responds to new and emerging issues by setting up working groups to examine them in-depth. Through the voluntary efforts of its members, and encouragement by Government, UKCCIS has achieved a lot over the years. We have:

- Rolled-out free, family-friendly filters for the vast majority of broadband customers with prompts to encourage parents to activate them.
- supported providers of social media and interactive services with a guide to encourage businesses to think about "safety by design" to help make their platforms safer for under 18
- Created advice for schools and colleges on how to respond to incidents of 'sexting'; and also guidance for school governors on online safety.

Something I am very excited about is new work that UKCCIS has just started on Digital Resilience. It brings together relevant stakeholders that represent the education sector, parents, industry, expert civil society organisations and children themselves. What do I mean by 'digital resilience'? Well, it's all those things we can do to stay safe around people we meet on the internet. Many of you may do it without thinking - sometimes it's common sense and sometimes it isn't. So we are looking at these areas and what help and advice is already out there. We want to see what more we need to do to improve how children and young people have the digital skills and emotional understanding to feel empowered to lead their digital lives safely. It's very ambitious work and it is through such focused working groups that the UKCCIS Board is able to respond to new and emerging issues. We are also looking at new and emerging technology so we can assess if they will have an impact on children and young people’s safety.

Another extremely important area of my work as joint Home Office Minister is combating the sexual exploitation of children online. The Government strongly supports the work of the Internet Watch Foundation in tackling illegal images, and recognises the work that the internet industry has done to make blocking a real success. But the sexual exploitation of children online cannot be dealt with by any one country, company or organisation working in isolation: a coordinated global response is needed to address this global threat.

With this in mind, the UK has brought together the We PROTECT Global Alliance to End Child Sexual Exploitation Online: a global coalition of countries, technology firms and organisations committed to national and global action to end the online sexual exploitation of children, working together to identify and safeguard more victims of this terrible crime and apprehend more perpetrators. It was launched in London nearly two years ago. Since then, it has merged with the Global Alliance Against Child Sexual Abuse Online. This has created, for the first time, a single global initiative with the expertise, influence and resources to transform how this crime is dealt with worldwide. By joining up our efforts across national borders, we can guarantee children the future that they deserve and secure their safety in the digital world.

I am really pleased the UK IGF is hosting a youth panel this year, and that they will have the opportunity to share their views with you on what everyone has been discussing today.

I want to leave you with a final thought. Since the global UN IGF started – eleven years now – the generation of under 18s has been quietly but steadily increasing their stake in the areas you are discussing today. Last year, the global UN IGF’s mandate was renewed for another ten years – can you imagine what this cohort will think of the internet then? They will be setting up businesses, programming with the same ease as they type text messages today, and coming up with the next generation of technology. Some might be following your footsteps and think about internet governance.

My appeal to you is to incorporate children and young people into your thinking. As you consider your areas of work, research for new trends, and as you wonder how technology will impact society in future, consider the interests of children and the opinions of young people. Help them participate in our journey because before you know it, they will be right next to you deciding about our future.

-- ENDS --

Plenary Four: An Internet for Children and Young People

Will Gardner (Childnet International), and Youth Panel from the Diana Award

(1) Will Gardner opened the session with a short introduction on Childnet International's remit, and asked the six panel members from the Diana Award, aged 14-18, to introduce themselves.

(2a) The first discussion tackled the topic on anonymity online. The youth panel balanced the benefits of anonymity – for instance someone from a conservative culture exploring their sexuality online through Tumblr – against the challenges this presents – for instance blurring the boundaries between banter and bullying by asking potentially inappropriate questions on ASKfm. One panellist noted that anonymity online makes people unaccountable for their actions, and therefore increases confidence.

(2b) The second discussion surrounded cyber-bulling and online friendship. The panel distinguished between online and real friends, but did not dismiss the advantages of spreading messages of support, meant for one online friend, but not unsuitable for dissemination across all Twitter followers. On a related theme, the panel commented on the pressure to respond to messages, especially on Snapchat, with the advent of read receptions.

(2c) Intertwined amongst the topics of anonymity and cyber-bulling laid a third topic, the use and suitability of blocking and reporting tools on social media. The panel expressed the view that they would block bullies rather than report them: although both systems are efficient as any bullying stops, reporting is ineffective since there are inadequate sanctions against the bully. The reporting policy of Facebook was held up as a preferred practice, because the anonymous reporter can expect a non-automated response within 24-48 hours, indicating what action has been taken.

(2d) One panellist offered an intervention on the fine line between freedom of speech and hate speech. Noting a study which suggested that one third of 12-15 year olds had encountered hate speech online, he opined that this was not acceptable, and suggested that celebrities can act as good role models by considering the impact of their tweets.

(2e) Next the panel considered the fourth topic of online safety education. Two educational experiences were compared: in an all girls' school, online education included issues such as sexting and harassment; in a state comprehensive, there was no formal education. Panellists described an age gap, that there was greater pressure in early secondary school, but that this subsided at GCSE and above, in addition to a generational gap, that their younger siblings have passed over Facebook in favour of Instagram and Snapchat. The panel were unperturbed with the use of internet filtering policies in schools.

(3) The final topic, internet policy, included a series of short questions from the floor. One panellist indicated the arbitrary requirement of being 13 to register on Facebook, and the ease with which a 'confirm 18' button can be clicked. In response to a question, another panellist noted that since young people cannot vote, social media in general – but particularly Twitter – is the primary way by which young people can have a voice and influence politics.

(4) Gardner thanked the panellists for their efforts, and Jean-Jacques Sahel (ICANN) suggested that perhaps young people should be represented on each panel next year.

Wrap Up

David Souter (Development Expert), and Andrew Puddephatt (Global Partners Digital)

(1) David Souter framed the day using three themes. The first, most significant these was changing standards, rules and norms: the current online environment is built on European rules and norms, although the Brexit decision makes the continuation of these norms uncertain; on privacy and identity, new rules and norms are required now data is collected by default; on politics online, the wider engagement in politics comes at the expense of norms of behaviour when engaging in political discourse. Second, Souter suggested that while there is a high degree of complexity and diversity of experience online, we almost universally continue to value privacy, want information, and fear cybercrime. Finally, Souter restated a point from Rt Hon Matt Hancock's speech; that the pace of technology exceeds the capacity of institution to adopt to it, before suggesting that multistakeholder engagement offers a partial remedy insofar as it ensures rules and norms are adaptive.

(2) Andrew Puddephatt continued, noting an increasing tendency toward dystopian perspectives regarding the economy, communication and politics online. He suggested that current discussions on the impacts of the internet are mired in assertion, rather than in the results of empirical studies. Gesturing toward Gutenberg and the importance of print, he speculated that the internet is more akin to oral communication, founded on rumour, gossip and the indistinguishability of fact; expanding on the latter, Puddephatt suggested that much like it took many generations to read and understand authored texts, it will take many generations to understand oral communications on the internet. Finally, he spoke to the difficulties that governments face in performing their role, both that governments do not know how to develop and impose rules, other than normatively; and that many, particularly non-western governments prefer bilateral or multilateral mechanisms when policymaking has the potential to impact upon the public interest.

(3) Souter expanded on the possibilities for the IGF. Although the IGF mandate was renewed in December 2015 for another decade, there remains the possibility for significant improvement, for instance by reducing the insider nature of multistakeholderism of the like-minded, by not oversimplifying discussion to the point of blandness, or by actively seeking to engage with other fora. Further, the IGF should actively solicit contributions from those involved in sustainable development, rather than merely engaging academics for their definitions; notwithstanding, the World Bank Development Report concluded that the internet has had less impact of development outcomes than was anticipated a decade ago, and second, that the internet has probably increased inequality in developing countries over the last decade. More generally, Souter offered three takeaways: that international cooperation is absolutely fundamental, that internet governance cannot be separated from geopolitics, and that the internet is internationalist, but geopolitics is not.

(4) Puddephatt closed the session out with some comments from an international perspective, following his dystopian theme. He noted that Russia increasingly asserts a Westphalian notion of sovereignty over the internet; that China are sending larger delegations to the ITU, ICANN and IETF, presumably with the long term goal of shaping the internet to a Chinese liking; that by contrast, President-elect Trump might not continue to send large US delegations to these international fora, or indeed push back against arguments in favour of treaty based arrangements. Puddephatt opined that we are moving away from global norms, toward an era of intense geopolitical competition, one outcome which might be an increase the importance of the ITU - whose approach to Digital Object Management indicates a different way of organising internet governance. Finally, he suggested that if the UK wants to prove itself as no longer in retreat from the world, perhaps one method would be to demonstrate leadership of a norms and rules based order.