November 2018
Geoff Huston

Has Internet Governance become Irrelevant?

A panel session has been scheduled at the forthcoming Internet Governance Forum (IGF) in Paris in November that speaks to the topic that Internet Governance is on a path to irrelevance. What's this all about?

Background

When the Internet outgrew its academic and research roots and gained some prominence and momentum in the broader telecommunications environment it found itself to be in opposition to many of the established practices of the international telecommunications arrangements and even in opposition to the principles that lie behind these arrangements. For many years, governments were being lectured that the Internet was "special", and to apply the same mechanisms of national telecommunications and trade regulations to the Internet may not wreck the entire Internet, but they would surely isolate the nation that was attempting to apply these unnatural acts.

Within this broad category was the notion that conventional means of conducting trade in services was not applicable to the Internet. While an early mantra of "The Internet must be free" quickly foundered when it encountered pragmatic realities, the next mantra of "Don't tax the Internet" gathered significant momentum. What was meant here was an admonition to governments not to attempt to unduly constrain the flow of data, as such actions would imperil the future value of the Internet.

But while the Internet might have been "special" in the 1990s, such a characterisation was unsustainable in the longer term. In 2003 and 2005 the United Nations hosted the two-part World Summit on the Information Society (WSIS). It was clear by the time of the millennium that the previous regime of national telephone operators and the treaties that governed the international aspects of this global service were rapidly becoming sidelined, if they had not been sidelined already. The Internet was sweeping all before it and each time it engaged with another sector it appeared to come out of the encounter as a clear victor. The Internet might still be special, but by the millennium it was recognised that it was not always special in a good way.

This WSIS summit was in the context of the emergence of the so-called information society and a recognition of a widening "digital divide" where richer nations were in an obvious position to exploit the possibilities that opened up with the combination of abundant computation and communications services and thereby amass further wealth, while poorer nations yet again found themselves on the other side of the divide. Far from being a tool to help equalise the inequities in our world by allowing all to access information, education and open global markets for their services, the Internet appeared to be yet another tool to further emphasise this divide between rich and poor.

The United States was a focal point in these discussions. At the time the Internet was still strongly associated with the United States, and the US had spent much of the previous decade both promoting its benefits and profiting from the revenues flowing into US companies. This promotion of the Internet and the free flow of information was certainly not without elements of self-interest on the part of the US, as it appeared that the interests of the new corporate behemoths of the Internet and the geo-political and geo-economic aspirations of the US appeared to have much in common.

However, it's often difficult to tackle the larger picture in these large-scale international forums, so it was no surprise to see attention turn to the individual elements that were contained within this picture. One of these

elements that became a topic of discussion in its own right was the status of the body that oversaw the Internet's protocol parameters, including the names and IP addresses, that are used as part of the central core of the Internet. This function, the Internet Assigned Numbers Authority (IANA) was originally part of the US Defence Advanced Research Project Agency's funded activities. After a few more changes within the US Government agency landscape responsibility for this function was shifted to a self-funded mode operated by a private sector entity, ICANN, with some level of US engagement remaining in place. This was variously portrayed as a control or as a safeguarding measure. Irrespective of the nature of the motivation, the result was that the National Telecommunications and Information Administration, part of the US Department of Commerce, oversaw a contract between the US government and ICANN regarding the operation of the IANA function.

At times perceptions matter, and the lingering perception here was that the Internet was still seen to be essentially under the control of a single sovereign state.

This unique US role was always going to be a problem for other nations. The international telephone and postal networks were governed by international treaty instruments that had been in place for more than a century. To have a single nation state positioned at the apex of this Internet structure was, to say the least, controversial. Naturally this was a major topic in 2003 at the first WSIS gathering. The UN Secretary General at the time, Kofi Annan, convened a Working Group on Internet Governance (WGIG), a grand title which either conflated this topic to an even greater level of prominence or appropriately stated its central importance to the entire set of concerns with the structure of the Internet at the time. Again, opinions vary here. There was no clear consensus coming out of this WGIG activity, and the 2005 WSIS gathering could not reach any form of agreement on this matter.

During the WSIS process the US apparently refused to consider any changes to its pivotal role in the management of the Internet's protocol parameters. The WSIS summit eventually agreed on a compromise approach that deferred any determination on this matter and instead decided to convene a series of meetings on the underlying policy principles relating to Internet Governance. Hence we saw the inauguration of a series of Internet Governance Forum (IGF) meetings. These forums were intended to be non-decisional forums for all stakeholders to debate the issues. Originally intended to be convened for a period of five years, culminating in the fifth IGF meeting in Vilnius, Lithuania in 2010, it has continued with two further five year extensions of its mandate, and the thirteenth IGF will take place in Paris, from 12 to 14 November 2018.

Internet Governance Forums

Even within its limited objectives the IGF would find it challenging to claim universal success in achieving its mission.

The IGF did not manage to address the underlying tensions relating to the pivotal position of the US in the Internet. In 2011 we saw the IBSA proposal (called IBSA because of a summit convened by India, Brazil and South Africa) for a UN committee in Internet Related Policy. In 2013, as a reaction to the US surveillance stories being publicly aired on Wikileaks, a number of Internet organisations, including ICANN, the RIRs and the IETF released the "Montevideo Statement" calling on the US to step back from its central role. The US surveillance disclosures also appeared to be a major factor in Brazil's sponsorship of the 2014 netMundial initiatives, which also appeared to have the support of ICANN. Once more the call was for the cessation of the US control over the Internet's protocol parameter function. At much the same time Edward Snowden released a set of material that documented how US agencies were undertaking of widespread surveillance using the Internet.

These Wikileaks and Snowden disclosures weakened US resolve, and in October 2016 the previously unthinkable happened. The US government signed away its functional role and passed control of the protocol parameter function to an independent ICANN.

If the IGF was the forum to discuss the public policy issues related to the privileged position of the US Government with respect to the Internet, then the principle rational for the IGF also finished in October 2016.

In theory at any rate the US no longer claimed the ability to place its finger on the scale with respect to the carriage of these matters.

On the other hand, this is perhaps a far too narrow a definition of the role and scope of the IGF. The IGF process has managed to gather a more sophisticated shared understanding of the layers within the Internet and the ways in which these various components both share common objectives and create tensions when competing to achieve similar objectives. The elements of carriage networks, consumer devices, servers and service delivery networks, applications, and application behaviours all operate in a semi-autonomous manner. The previous model of the locus of control of an entire service environment sitting within the telephone company within each nation state was not repeated with the Internet. The Internet has exposed each of the various component service activities as discrete activities, and instead of orchestrating these components within the framework of the procurement processes of the larger service entity, a variety of new markets have been exposed: technology standards, fibre and mobile services, computers in all forms from handsets to servers, applications, service providers and content publishers all operate semi-autonomously, and the orchestration of their actions is through markets and market interactions. The Internet is not operated by a single service delivery company, nor is it a defined destination. It is a series of inter-twined markets. The implication for governance processes was profound, and the IGF has managed to both expose this change and steer a constructive path of commentary and dialogue on these changes as they have happened.

Internet Governance Today

I'd like to nominate three major themes of national and international interest in today's Internet that have some relevance to the topic of Internet governance.

The first is the issues that can be summarised as the "digital divide." There are still the haves and have nots across the full spectrum of our world. The digital divide is as big as it ever was and there is no visible movement in directions that would ameliorate the societal impacts of these changes. If anything, this divide has further broadened in scope. In absolute terms it may be the case that more individuals have some form of Internet access than was thought could possibly be achieved even 10 years ago. But today that's still only one half of the world's population, and the other three billion people are isolated from the mainsteam. The divide also operates across other dimensions, including the cost of access, the quality and speed of access, the accessibility of information, the extent to which goods, services and information are accessible using a local language. They all form subtle aspects and not so subtle aspects of digital exclusion.

The second theme is also not a new theme, but it has dramatically increased in importance in the past two decades. Its components have various labels, including Cyber Security, Malware, Abuse, Spam and Viruses. It can be summarised in the observation that today's Internet is a toxic place that not only provides haven for various criminal and fraudulent activities but also provides haven for darker actions encompassing the current set of concerns relating to terrorism and cyber-offensive tactics from state-based actors. The uncomfortable observation is that technology-based counter-measures may be failing us and the fabric of our society seems to be very vulnerable to concerted hostile cyber-attack. We've adopted strong encryption in many parts of the environment as a means of protecting users against various forms of organised surveillance, but in so doing we've turned off the lighting that would otherwise expose various acts of malfeasance to our law enforcement bodies. We have had to make some tough decisions about balancing personal privacy and open attribution. But this lack of clear attribution and greater ability to embed communications behind strong encryption means that various forms of policing this digital world has become expensive, frustrating and ultimately very selective in its application.

The third theme lies within the changes occurring within the Internet itself. In recent years we've seen the proliferation of content distribution networks that attempt to position all of the data and services that any user would request as close as possible to the user. It used to be the role of the network to bring the user to the content portal, whereas these days we are seeing content shifting itself ever closer to the user. In and of itself that's a relatively significant change to the Internet. The public carriage component of the Internet is shrinking and being replaced by private feeder networks that service these rapidly expanding Content Distribution Networks (CDNs). The bigger question concerns the residual need for global names and addresses in this

CDN-centric environment. The Internet is no longer a telecommunications network that carriers user traffic across a common network. Today's Internet is a content distribution network that is very similar to a television broadcast network where the transmission component is limited to the last mile access network. The essential difference here is that on the Internet each user can define their own program.

One possible response to these concerns is the perception that these situations are instances of collective failure of the Internet Governance framework. Allowing the private sector unfettered control of the public communications space has produced very mixed results. Yes, the obsessive concern with catering precisely to what users want has produced a remarkably efficient and capable supply chain that can bring the economies of massive scale to market of a single unit, and this is a modern-day marvel. But at the same time the private sector is largely uninterested in the general health and welfare of the larger environment and the Internet appears to be the victim of such collective neglect.

The public sector's forbearance with the cavalier attitude shown by various Internet players may be reaching a breaking point. The EU initiative with General Data Protection Regulation (GDPR) is a clear signal that the honeymoon with technology is over and various national regimes clearly want to see a more responsible and responsive attitude from these players to public concerns. Doubtless we will continue to see fines being set at levels intended to be eye-watering for even the largest of players. While this measure has the unintended side-effect of eliminating the smaller players from the market and potentially stifling competition, a major public sector goal is to bring some sense of broader social responsibility back to the major players. This regulatory stance will no doubt continue in both the EU and in many other regimes.

But is this increased national engagement a failure of the Internet Governance framework or a more conventional role of public sector regulation of a market? Private corporate entities have a primary duty to their shareholders, and do not necessarily have the same over-arching obligation to the public good. If self-interest and public interest coincide, then that is a wonderful coincidence of fortune, but when they differ, corporate self-interest necessarily wins. It is naive to expect that any messages of constraint and prudence to the private sector would be heeded unless it has the authority of regulatory impost with some form of punitive enforcement measure.

If governments are feeling emboldened to enact regulatory measures for an industry that until now enjoyed some level of immunity from conventional social responsibilities, then how do these same governments feel about the actors that look after the elements of Internet infrastructure?

IANA and its Fellow Travellers

A highly visible part of the US position with respect to the Internet was the defining of the IANA function as an activity performed under the aegis of the US Government by a contracted agency. There are three activities that are loosely bound within the IANA role. They encompass the carriage of Internet addresses, Domain Names and IP protocol parameters. Let's quickly look at the current position of these three activities, and look at their relationship to the Internet Governance dialogue.

The IETF started in the late 1980's with all the youthful hubris and enthusiasm of any new entrant to the field of technology standards. Loudly criticising the staid incumbent standards bodies as being production factories of "paperware about vapourware," the IETF paraded its difference loudly and proudly. The IETF was motivated by a determination to quickly produce specifications that allowed for interoperable implementations of useful functions as its prime role. They "rejected Kings, Presidents and voting, and believed in rough consensus and running code." They were not there to create standard specifications from offered technology but saw themselves as the architects and engineers of the Internet. Their self-perception of their role was to develop technology, and do so quickly and efficiently,

As the IETF matured it became more like many other technology standards bodies, but there have been moments when the spark of the early days has returned. The IETF's reaction to the Snowden leaks was to regard the surveillance actions of national security agencies as a form of attack on the IETF's protocols. The response was one of taking the IETF's protocols and adding strong encryption wherever possible. The results

have been rapid and profound. The web now uses encryption as the de facto standard. The IETF has produced standards that encrypt mail, messaging, and even time synchronisation. They have been thorough in taking even the last vestiges of traceable information and defining ways to encrypting it.

But at the same time the IETF has not been able to provide a technology solution to all perceived issues and problems relating to abuse of the Internet's technology. If SPAM was a technology battle, then the IETF has lost it. No matter what the latest solution has been over the past two decades, the spammers have been able to work around it. The disturbing Denial of Service attack space is another illustration of how it is possible to turn these technologies around and turn them into attack vehicles. There is a pervasive feeling of vulnerability and a sense that technology-based solutions are not offering the needed reassurance. These are hard problems and it is completely unfair to suggest that the IETF is responsible for these issues, and unfair to believe that the IETF should've had a solution to each and every one of them. However, the IETF was adamant in the past in saying to others "leave us alone, we know what we are doing." That was, as it has turned out, a bit of a stretch! Our protocols are not resilient enough and we are now seeing players break away to create their own protocols without necessary seeking IETF permission.

What about ICANN and the Domain Name System?

It's challenging to summarise the issues into a couple of short paragraphs, but one could trace much of the name space issues back to the original concepts in the early days of the Internet that adopted a hierarchical name space with a deliberately small set of top-level names. Country codes were added to this name set, but at the same time these "stateless" names continued. So-called "Name Envy" quickly followed as others wanted to reap the benefits of these generic top-level domain names and the pressure to add more such names to the DNS has continued ever since.

However, there is a contrary view that whatever the Internet may need today, more generic top-level domain names are not on the list of actions that would help the Internet. As we see more of these top-level domain names added into the root zone, we see more domain names that have little intrinsic value. There is a widespread perception that these new generic top-level domains represent havens of online abuse and malfeasance. ICANN, as the policy forum that has the carriage of stewardship of the name space, appears to be largely impotent in being able to stop this behaviour and incapable of stopping itself from allowing applicants to pay ICANN large sums of money to generate even more such unnecessary top-level domain names.

Where does this end? We know that we cannot support a DNS infrastructure with billions of names in the root zone. But precisely how many we could support before the DNS system starts to fall apart is an unknown number. Rather than simply stopping this process of adding more top-level domains and working within the parameters of what we have, ICANN appears to be set on an inexorable path to expand the root zone of the DNS and do so without any endpoint in sight. There is no sense of constraint in their activities, and one wonders if the only point of constraint is the point when we've managed to completely destroy the utility of the DNS and its name system.

What about the Regional Internet Registries and the Internet's address infrastructure?

The run-down of the address pools associated with IPv4 was a surprise to many. It's hard to see this as a fault in the RIR's carriage of the administration of the address space, but it is seen as a larger systemic failure. The IETF had identified the forthcoming exhaustion of the IPv4 address space as an issue almost thirty years ago, and to avoid this scenario it designed a protocol that had a vastly larger address space to accommodate future growth. Following this IETF lead, the Internet industry was meant to have behaved prudently and transitioned to use IPv6 long before IPv4 had run out. Obviously, this has not happened, and we are still largely using IPv4 long after the run-down of available IPv4 address pools.

But perhaps while it is challenging to make a case this this represented as fault in the RIR's function, the IETF does not escape some level of criticism here. In defining IPv6, the IETF ignored of the primary drivers of the success of a network, commonly described as "connectivity is its own reward" and produced a protocol that was incompatible with its predecessor, thereby defining an entirely new network. Now, a system where growth

is proportional to its size is the definition of exponential growth and after years of IPv4 Internet the new network faced an impossible chase. The RIRs, as stewards of the distribution of number resources, have no capacity to coerce the adoption of this new protocol in any way that is sufficient to ensure its immediate deployment. Instead, the entire transition is a protracted waiting game with no obvious end in sight.

Is Internet Governance Irrelevant?

I'd like to think it's not the case. I'd like to think that the principles of an open and accessible technology foundation are an intrinsic component of open accessible and healthy societies. I'd like to think that the principles of accessibility, transparency and diversity that are part of the mode of operation of the IGF are valuable principles and should ensure a healthy and robust debate on the various topics of Internet governance. I believe that the IGF has been of assistance to the increasing level of shared understanding of the Internet, in both its strengths and its weaknesses. I suspect that Internet Governance will be irrelevant only when we let it become so. Like any open cooperative effort, it requires continual care and attention if it is to continue to flourish.

But there is another side to an answer to this question. We are embarking on changes in our society which are as dramatic and even as traumatic as the industrial revolution. Such revolutions leave a path of social dislocation and uncertainty in their wake, and this information revolution is no exception. It is perhaps unsurprising that nation states tend to be more assertive in such situations as they try and mitigate some of the worst excesses of such social disruptions. One side-effect of this increasing nationalistic stance is that the various international efforts, both regional and global, tend to be regarded with increasing levels of distrust from these national regimes. In times of uncertainty and stress nations naturally try to raise the drawbridge and attempt to insulate themselves from such disruptions by asserting greater levels of control within their own national realm.

The industrial revolution was certainly triggered by the refinement of the steam engine, but the social revolution was far larger in scope than the invention of a simple mechanical device. In a similar line of thought, maybe it's not the Internet or its governance that lies at the heart of many of today's issues. Maybe it's the broader issues of our enthusiastic adoption of computing and communications that form a propulsive force for change in today's world.

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

Author

Geoff Huston B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net