The ISP Column
A column on various things Internet

April 2025
Geoff Huston

Internet Governance - The End of Multi-Stakeholderism?

When the Internet outgrew its academic and research roots and gained some prominence and momentum in the broader telecommunications environment its proponents found themselves 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 might not wreck the entire Internet, but they would surely isolate the nation that was attempting to apply these measures.

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 of trying to pay the bills, 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 with taxes and related imposts, as such actions applied in a careless manner was likely imperil the future value of the Internet. This was a unique opportunity to take the role of public communications away from the sclerotic and bloated telephone monopolies and apply some of the vibrant innovative energy that was driving the computer industry into the communications realm.

But while the Internet might have had some claim to exceptionalism in the 1990s, such a characterisation was unsustainable in the longer term. 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 had been sidelined. The Internet was sweeping all before it and each time it engaged with another sector it appeared to emerge from the encounter as a clear victor. The Internet might still be exceptional, but by the millennium it was recognised that it was not always exceptional in a good way. In 2003 and 2005 the United Nations hosted the two-part World Summit on the Information Society (WSIS) to try and come to terms with these changes, and ideally to try to ensure that all economies would benefit from this revolution in computing and communications.

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 entrench 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 that were early adopters of Internet-based services. 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 newly emerging 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.

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, the United States.

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 that would discuss on the underlying policy principles relating to Internet Governance. 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 a further five-year extension of its mandate, and then a ten-year extension, culminating with the forthcoming IGF meeting in Norway at the end of June 2025.

Internet Governance Forums

Even within its limited objectives of being a forum for little other than talk 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 still 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 might be able to 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 four 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.

But when we talk of a *digital divide* we can broaden our view and look at the position of the world's most valuable digital enterprises, namely Apple, Microsoft, Nvidia, Amazon, Alphabet and Meta, which have a market capitalisation of some 12 trillion USD (just before the recent Trump-induced stock meltdown). The aggregate position of these six enterprises is so large and so powerful that everybody else, individuals, corporates and most governments, find themselves on the impotent side of this digital divide.

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 have become expensive, frustrating and ultimately very selective in its application. There is also the observation that these digital megaliths have made vast profits from their dominant position, while at the same time they have managed to transfer the costs of large-scale deployment of poor quality software and tools back on the public sector.

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 failure of 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?

Rebuilding National Barriers

The recent erratic moves by the US President to initiate a trade war on a global scale will have far-reaching implications far beyond stock markets and will inevitably include the digital world and what we refer to as Internet Governance. The US moves on the unilateral imposition of tariffs can be interpreted as a vote of no confidence in global trade and open markets by the US, and a resurgence of a theme of strategic national self-reliance in all areas of economic activity, including the digital realm.

The question of course is how will others react?

> This week I saw a notice from a DNS hosting provider relating to hosting Russian domain names:
>
> "We are contacting you about a recent communication from the Russian Federal Service for Supervision in Communications and Information Technologies and Mass Media (Roskomnadzor).
>
> This relates to the potential future restrictions on foreign hosting providers and the need for domain administrators who use foreign DNS infrastructure to transition to Russian hosting providers listed in the official register."

There is a visible concern in many national regimes that large amounts of their digital infrastructure are being operated by foreign enterprises, and by "foreign" it is more often than not simply "US".

Today's deregulated digital communications environment is held together by commercial contracts and the extent to which such arrangements can be torn asunder by seemingly erratic US

presidential edicts no doubt causes many to lose sleep! In a bad case scenario, can these US entities be coopted to hold a country's digital infrastructure hostage as part of the "art" of a national trade deal? In the extreme worst-case scenario, can these entities be forced to operate in an overtly hostile and disruptive manner in terms of services provided to foreign entities? What happens in a modern national digital economy when its infrastructure underpinnings are deliberately sabotaged by such entities acting under duress from some form of executive order?

The order in which we operate the Internet today is held apart from the conventional treaty body for communications (the International Telecommunications Union, or ITU) because the US administration in the late 1990's under President Clinton led a coalition of friendly economies notably Australia, Canada, Japan, and the EU in supporting the move to recognise a private institution to perform the allocation and administration functions for internet infrastructure elements (notably names and addresses) based on what we came to call "multi-stakeholderism. The US recognition of this form of industry self-regulatory governance was more like an insubstantive veneer for many years, as the US administration (in the guise of the NTIA within the Department of Commerce) performed an oversight role of the root zone of the DNS in the background. However, as we've already noted, the US administration backed out of this oversight role around a decade ago and has largely disengaged, being unwilling to continue to pay the diplomatic price of being the backstop in holding this coalition together in the face of large-scale devaluation of US international diplomatic capital by the Wiki Leaks and Snowden incidents.

You could argue that by 2020 the job was done in any case. The "value" of the Internet was tightly held by a small elite of truly massive US enterprises and any role of the US administration to support these enterprises in the international realm was no longer necessary. Other countries have been willing to go along with these arrangements for a variety of reasons - there was the ill-defined promise of digital prosperity and other national communities could benefit from this shift to digital infrastructure as well.

But the distribution of wealth and social power in this "new" world is vastly different from the old industrial world. Having valuable digital enterprises domiciled in a nation does not translate to widespread economic prosperity. The digital enterprise does not rely on large workforces, and the immense concentration of wealth often results in inventive efforts to avoid conventional forms of corporate taxation by the state. The issue is that the distribution of this digital wealth is very uneven and while a small clique of individuals may live in an extreme level of opulence, large proportions of domestic populations are disenfranchised and marginalised.

Not unsurprisingly, we are now seeing a response to this situation, in the form of a wave of populism gain social power in many national communities: Not just in the US, but in Germany, France, Hungary, the UK and other western economies. Such populism is based in part on restoring an old-world order that "protects" national economies and eschews many forms of globalism.

At the moment this is being expressed in various ways in a visible shift to national compartmentalism, not only in limiting the cross-border flow of physical goods through the imposition of punitive tariffs, but in the efforts to contain digital assets and infrastructure roles to national entities, domiciled within national boundaries.

Obviously, this is not looking good for the Internet. It is increasingly likely that we will return to an order where international dealings are strictly defined through the use of a myriad of regulations overseen by treaty-based organisations. It's extremely challenging to espouse the benefits of an

open multi-stakeholder global communications environment when the dream has been so basely corrupted by the exploitative excesses of the small clique of digital megaliths.

The year 2025 is particularly challenging when WSIS+20 is reopening the basic debate about the merits of multi-stakeholderism. "National Internet Sovreignity" is a powerful meme these days and multi-lateralism, as compared to multi-stakeholderism, has a seductive appearance of addressing demands for greater levels of national autonomy, particularly in communities where populism is a dominant social force. This debate is taking part in an environment when the change in the stance of the US administration has effectively torn up all the old order. It is unclear as to how (or even whether) the US will continue to expend effort to support multi-stakeholderism, and the erratic record of the US on the recent topic of tariffs lends further credence to the stance that the US in no longer a widely trusted and stable advocate of the benefits of multi-stakeholderism in the international realm.

In mid-2024 we saw efforts by others national entities (AUDA for .au, CIRA for .ca, InternetNZ for .nz, and Nominet for .uk) to create a coalition to speak up for mult-stakeholderism (A Technical Community Coalition for Multistakeholderism (TCCM) is evidence of others attempting to fill this clear gap. Notable is the absence of the US.

I wish this group well, but it is extremely challenging to make the case that today's international climate is in their favour. Given the huge issues in cyber-vulnerabilities, the entrenched position of US megalithic digital corporates, and the extremely erratic position of the US administration at present, the case that the ideals of the Internet that were espoused in WSIS some 20 years ago, and the promises of multi-stakeholderism in the development of digital economies where everyone benefits are still realistic prospects today is extremely hard to make. It's far easier to observe that we gave it a try and Alphabet, Microsoft, Amazon and Meta should be grateful to us for enabling their rapid rise to global dominance.

To come?

I can't help but feel very pessimistic about the coming years. The attempt to coopt private enterprises to work in a manner that safeguards the public interest in our common public telecommunications realm has failed, again. It reminds me of Theodore Vail's efforts in the early 20th century to do a deal with the US Congress to bestow on AT&T a monopoly in national telephone services in exchange for an undertaking that the company would act with restraint as an enlightened private sector entity that would act in the national public interest. As it turned out AT&T could not resist itself from exploiting its monopoly position for any more than a decade!

It looks like national pressures are calling an end to multi-stakeholderism in Internet Governance, hastened by a tectonic shift in the position of the US in international circles. The most likely direction we will now pursue in Internet Governance is a shift to multi-laterism and an increased role for the United Nations and the World Trade Organisation for the middle-ranked nation states, accompanied by a tumultuous period of US unilaterism.

Is this all due to the outcome of the 2024 US Presidential election? If there had been different candidates and a different election outcome, would the position we find ourselves be in today be materially different?

It seems to me that there are much larger social forces at play that transcend individuals and their actions, however erratic they may be! We are embarking on changes in our society which are as dramatic and even as traumatic as the industrial revolution of the nineteenth century. Such revolutions leave a trail 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 various international institutions, both regional and global, tend to be regarded with increasing levels of distrust from these national regimes and from populist national fora. 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 root cause of all social dislocation is attributed to the actions of foreign bodies and they claim that greater levels of national determinism will restore some aspect of a myth of prior national greatness and prosperity.

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 has formed a propulsive force for widespread social dislocation 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 AM, M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net