The ISP Column

A column on various things Internet

March 2024
Geoff Huston

Opinion: Digital Sovereignty and Internet Standards

There have been a number of occasions when the Internet Engineering Task Force (IETF) has made a principled decision upholding users' expectations of privacy in their use of IETF-standardised technologies. (Either that, or they were applying their own somewhat liberal collective bias and to the technologies they were working on!) The first major such incident that I can recall is the IETF's response to the US CALEA (https://www.fcc.gov/calea) measures. Some US Law Enforcement Agencies (LEAs) wanted an IETF standard for the provision of tap points in media gateway controllers. After much debate, and just a little bit of IETF angst, the IETF decided not to undertake any further standards work in this area (https://www.ietf.org/proceedings/57/slides/plenary-10.pdf, IETF 57, 2003). At the time, the IETF was still finding its way as a recognised international standards body, and such matters were largely seen by IETF participants through the lens of US domestic issues.

The conventional LEA position was that networks were used as a convenient and effective means to eavesdrop on the activities of individuals' activities, and such access to the network was enshrined in various regulation-sanctioned measures. But there were some rather large loopholes in this arrangement. The rights of citizens are recognised in many national democratic regimes, where eavesdropping orders typically require some level of approval from the judiciary. However, when the activities of aliens (non-citizens) are the subject of LEA investigation, the oversight process is somewhat different, if it even exists at all. The Snowden documents (https://grid.glendon.yorku.ca/exhibits/show/welcome-to-the-snowden-digital) revealed a situation in the US where the NSA had documented its efforts to take this eavesdropping to entirely unprecedented levels of scale and scope, and managed to sweep up both citizens and aliens in its amassing of data.

The actions of the IETF in response to the Snowden revelations were also taken to a new level. The IETF went further than simply not progressing standards relating to eavesdropping capabilities in network. They changed to an active role and embarked on a program of encrypting as much as possible of the communications protocols described in IETF standards (RFC 7258, "Pervasive Monitoring Is an Attack", May 2014). The IETF program is still underway a decade later, and while much has been achieved, there is still much to do.

Today, the overwhelming majority of the traffic being carried on the public Internet is now encrypted (https://2024.apricot.net/assets/files/APIC378/the-internet-and-cdn_1709097576.pdf, Bart van de Velde, February 2024). Not only is web related content traffic encrypted, but there are also now IETF-published standard mechanisms to encrypt DNS queries and responses. Work continues to seal up further portholes in the network. The QUIC protocol has pulled the entire transport control parameters into the encrypted envelope. In all of these measures there were still two points that could observe the entire network transaction in the clear, namely the two endpoints. Even this is now being sealed up. The technologies of "obfuscation", such as MASQUE, provide assurance that there is no single point in the network, nor within the server, are necessarily aware of both the content of the transaction and the identity of the client. This approach of combining encryption and obfuscation has been used in Apple's Private Relay service. Work continues in encrypting the initial handshake in the Transport Layer Security (TLS) protocol, the Server Name Indication (SNI), the final open porthole in TLS. Google's Chrome browser, the dominant browser across the entire Internet, is increasingly reticent to connect to a site that is not using TLS to encrypt the session.

From the LEA's perspective, a once stable arrangement between various public carriage service providers and local LEAs was being fundamentally disrupted by the IETF's reaction to the material revealed in the Snowden papers. This shift to the general use of encryption in Internet transactions also shut out network operators, making much of the network's traffic opaque to operators.

The message to the LEAs appeared to be clear: If you didn't like what the IETF was doing to the Internet then it was time to head to the IETF yourself and advocate a more moderate stance.

From a non-US perspective, and notably from a European perspective, the message was even more stark. All this was generally perceived as a US situation of overly zealous US agencies taking the gathering of network data about users and their activities to unprecedented levels and the IETF taking a position in response that appeared to be verging on the hysterical. But there was another element here. Not only was this IETF position frustrating various LEA network eavesdropping efforts, but this also appeared to be an effort by a small collection of mainly US-based technology and service providers seizing control of the entire Internet. The extensive use of encryption not only shut out network-level eavesdropping, but it also acted as a dampening factor to competitive access to the network. The shift from a formerly open network to one that was closed behind an encryption wall also marks a perceived shift to a network that is even more resistant to open competitive access. Given the almost complete domination of the Internet market by US entities already, the EU seems to have been left behind by the Internet. In the digital economy they are the clients, not the providers. Or in the terms of the old world of imperial empires, they are the new outpost colonies of the Digital Imperium, and certainly no longer the Head Office.

I'm sure that for many politicians and bureaucrats in the EU, it would feel that their digital sovereignty has been comprehensively undermined over the past decade and it is now held captive within what they see as largely US issues that have been inflated into an international context. How can they push back on this situation, and assume a more active role within the Internet, and shift a greater proportion of revenues from the digital economy away from the US and towards EU entities?

It is possible to construct a case that digital sovereignty assumptions are being challenged as a result of the Internet's standardisation activities. It appears that these industry-based bodies, and most notably the IETF, have control over much of the digital technology agenda, and the manner of their orchestration of industry responses is not only in the collective actions to evolve the nature of digital services in particular directions by industry providers, but also to gather collective support for such directions through the standards setting process. The natural corollary of this view is that if you want to influence this technology agenda, to, for example, instil some consideration of how human rights might be impacted by a technology, or some to exert some influence on the balance of individual and societal interests in the formulation of digital technologies, then you need to exert influence the actions of such standards bodies. Pragmatically this means sending your own advocates to the IETF, the W3C, the IEEE and similar. If these new generation digital world standards bodies are unwilling to recognise the primacy of the international treaty body, then ITU-T, in all matters concerning international telecommunications, then the only remaining recourse is to attempt to exert influence by exploiting their own propositions of open participation. Put simply, its time more public sector folk showed up at the IETF. Or, from the EU perspective, it's time the EU sent its own people to IETF meetings! (https://openfuture.pubpub.org/pub/internet-standards/release/2).

Really?

As a long term active IETF participant with some experience in chairing IETF Working Groups and also had experience as a member of the Internet Architecture Board for some years, it is disconcerting for me to hear the IETF being ascribed with such levels of power and influence in the international political arena. The IETF's role in generating standard profiles of technology is to assist in the production of interoperable goods and services. These standard specifications have no inherent force of adherence. Standards are intended to be used as an aid to consumers of such goods and services to frame their expectations that such goods and services are fit for purpose and interoperate with similarly standards-conformant services.

You might think that a focus on providing assurance to consumers about the quality of vendors' products would motivate consumers act collectively to develop such standard specifications, but in the inverted world of Internet technology it is the vendors who have controlled the IETF's standards process (https://archive.psg.com/051000.ccr-ivtf.pdf). These vendors appear to have used the standards process as a forcing function to drive complexity into technology specifications with the desired outcome of creating barriers to entry in an otherwise competitive market. These vendors were not necessarily pursuing any particular social or political agenda. They were simply following a more banal path of attempting to leverage some advantage for themselves as incumbent vendors in a competitive scenario.

Most national regimes already have a rich framework of measures to protect consumers from abuse through market distortions, whether its abuse of market power by dominant providers, or just plain misbehaviour! If the public sector is finding it challenging to address such market distortions within the Internet through existing measures, then why would standards make their role any easier? Why would direct participation in an industry-based technology standards-making forum, such as the IETF, provide the means for a nation state to assert its digital sovereignty?

This appears to me to be a case of inflating the role of standards to a level that is completely disconnected with the rather mundane role of such technology standards. How did we get to this point? Why is there such a difference in perspectives of the role of standards in a deregulated domain between the US and the EU?

Looking Back

I believe that this has much to do with the early days of the telephone industry. Immediately following the unveiling of the telephone at the 1876 World Expo there was a mad scramble to set up companies to deploy telephone networks. Mirroring the euphoric days of the Internet Service Provider explosion in the 1990's, there were hundreds of small telephone companies across the world within a decade or two. The problem here was they did not interconnect and did not provide a cohesive service. the more people or businesses you wanted to communicate with the more telephone handsets you needed to install. The process of rationalisation of this nascent telephone industry was brutal. Most national regimes nationalised the telephone service, cutting out these early entrepreneurs, and in its place constructing a single national service. This did not happen in the United States. Theodore Vail, the head of AT&T managed to sway the US Congress that they could have a national telephone service without touching the national financial purse by granting a national monopoly to AT&T. In the Kingsbury Commitment of 1913, AT&T undertook to be an enlightened private sector public utility operator for the nation.

The telephone developed slowly for some decades, but the direction was inexorable. The telephone network was being steadily reconstructed first as a switching and multiplexing network, and then as a digital switching network. The invention of the transistor (Bell Labs, AT&T's research laboratory) and its subsequent refinement into the integrated circuit not only heralded the computer industry, but the led to the integration of computing capabilities into the telephone network, which naturally changed the economics of the telephone industry. A digital telephone network was substantially cheaper to operate, while consumers were used to paying the same costs for making calls. The telephone companies became large scale revenue generators for their respective national economies. In the US the privileged position of AT&T was under threat, directly aligned to the increasing profitability of telephony in the dawning digital age. The US State Department filed an antitrust case against AT&T in 1974. As with many aspects of US communications policy, the matter was decided by US courts. By virtue of a consent decree in 1982, the US telephone industry was deregulated in the US, and effectively opened up to competition.

It wasn't just the downward shift in the cost base of the telephone service that was the catalyst for fundamental change in the telephone industry. The early telephone environment was a collection of national networks, and it was not until the opening of the international system through subscriber international dial services that these systems were forced to address their differences. AT&T found itself in an anomalous position internationally. In a room of some 150 other government-operated national telephone network operators where decisions were taken by national votes, AT&T found itself increasingly isolated. For example, while other governments could perhaps tolerate the structural inequities of the international call accounting financial settlements as just another form of international financial aid from rich economies to not so well-off national economies, AT&T did not appreciate being compelled to be a significant donor of international financial aid. AT&T strongly felt that that this was a role for governments, not private sector entities.

AT&T was looking for a way out of these ITU-T imposed arrangements, as they apparently felt that this was little more than institutionalized international extortion. As a result of concerted p[political lobbying on the part of AT&T, when the Internet's ascension was looking more certain, there was a concerted effort from the US to withhold the Internet from the ITU-T and instead place the Internet on a foundation of deregulation and competitive market activity. In taking up AT&T's agenda, the US position with respect to the Internet was to treat this activity in the same manner as the newly deregulated US telephone space, where the discipline of market competition would create efficient outcomes. In such an environment the Internet-based successors of AT&T would not find themselves outvoted in a Geneva room populated by an overwhelming majority of government representatives. The economic heft of US enterprises, and their strong lead in technology would place US commercial interests in a paramount position in this new market-driven international telecommunications domain.

This technology leadership position has duly played out over the ensuring two decades into a "winner takes all" market outcome. The small collection of digital behemoths that dominate the digital space with their content distribution platforms are all US-based enterprises these days.

The market-driven approach to oversight in this sector has not proved to be an overly effective one for the public sector outside the US. The outcomes of this policy to date have achieved little other than reinforce the defacto global hegemony of a handful of US digital service platform enterprises, namely Alphabet, Amazon, Apple, Microsoft and Meta.

Digital Sovereignty

We are now seeing in the EU the emergence of the assertion of *digital sovereignty*, which espouses the approach that states should actively assert their authority and protect their ability to undertake self-determination of policies and practices in the digital sphere. This shift has led to more forceful attempts to curb the market power of these large technology companies over European digital markets and introduce greater levels of accountability. These measures such as the GDPR and the EU Data Act, illustrate an increasing EU effort to also influence the direction of digital technology, asserting that the individual's fundamental right to have their data protected, and that commercial activities should respect the primacy of such privacy and protection considerations.

One view here is that Internet standards, and the IETF in particular, are at the centre of many corporate and national strategies to exert broad influence and shape the internet to match their own preferred image. This view asserts that standards have become the most important component of the Internet's infrastructure. Due to their economic and strategic importance, the process of creation of internet standards are inevitably subject to the intense economic and political tensions between diverse world views.

I think the reasoning behind this view is somewhat flawed. It ascribes to the IETF a degree of influence of the technical direction of the Internet and digital technology which is completely unfounded. Yes, it’s true that the IETF works on reflects the current needs (and even aspirations) of many of the technology providers and vendors in in this space, but the IETF is not necessarily the thought leader here. It merely reflects the current needs and desires of the industry actors that play in the IETF’s space. After some decades of participation and close observation, my view is that the IETF’s strengths lie in open and unsparing peer review of technology proposals. What is important is that this is not a process of trying to assemble an outcome specification that is so anodyne and meaningless that there is nothing left for anyone to object to by virtue of there being nothing left in the specification in the first place. Nor is the outcome weakened by trying to compromise between diametrically opposed views (the choice of a 48-byte ATM payload comes to mind as one of the worse cases of such compromises). What is important in the IETF review process is a resultant specification that is coherent, safe to use, and can be used to generate interoperable working implementations.

From this perspective, parachuting more civil society folk, and more political folk into the IETF standards-making process is only of intrinsic value if the objective is to disrupt the standards-making process and ensure the eventual transformation of the IETF into a devalued role of irrelevance to industry it services with standards!

By virtue of its industry base the IETF is a timely reflection of the current desires (or even current obsessions) of industry actors. But one should be careful to distinguish between the primary source and its various reflections.

Yes, I know many state actors are basically uncomfortable with today's picture of overarching global dominance by a handful of US entities who appear to be operating in a totally unaccountable manner. There is a cyber-vulnerability situation which is running totally out of control. There is a so-called security framework which is largely useless. And now the industry is pursuing an encryption agenda which appears to frustrate the efforts of most law enforcement bodies to try and engage with this abusive behaviour. Every state actor wants to head to a forum where the industry players gather and try and put the case that their current obsession with universal encryption and obfuscation is now damaging a broader agenda of advancing digital safety for citizens and enterprises. And I sympathise with that desire, but it's clear (to me at any rate) that a standards body is not such a forum where such a dialogue can take place. Standard specifications are an outcome, not a triggering motivation. Standards do not carry an agenda of charting the strategic direction of a market but document the consensus of the common positions taken by suppliers that support a profile of interoperability between suppliers.

The issue here is that the withholding of the Internet from the purview of the ITU-T, left no replacement for the role of the ITU-T as an international treaty body where signatory nation states have made binding undertakings. The problem is that no such comparable body exists for the Internet. That does not mean that the Internet is absolutely fine and would not benefit from various form of active coordination and an associated framework obligations by state actors. Far from it. Aside from the issue of market skew in the form of strong centrality in many aspects of service delivery, there is the issue of cyber insecurity and the ongoing hostility of the Internet, the fragmentation of the service and infrastructure environment, the woeful state of tools that offer trust and authenticity through to the basics of routing security and address integrity. There are many issues with today's Internet but getting the various actors to admit to an obligation that extends beyond servicing the immediate needs of their customer base to nurture this common space of the Internet's infrastructure has proved to be highly challenging, particularly if the only leverage is competitive market pressures.

Would this picture change if state actors were to attempt to exert pressure on the IETF to impose behaviours on various market actors though the leverage of standards? This strikes me as a far-fetched proposition. There have been many operational standards which have been ignored for years. BCP 38 is perhaps a classic example. The issue is that in a deregulated environment the actions of each actor align with their perspective of self-interest. Unless backed up by some external pressure to adopt, its going nowhere.

For a quite some time people showed up at ICANN meetings, mistaking ICANN's extremely focussed role of stewardship of the root zone of the DNS with some broader role of the regulator of the entire Internet. I'm not sure after many years that ICANN has been successful in convincing folk of its limited remit.

By shedding itself of many controversial roles, such as the stewardship of the root zone of the DNS, and the management of the process of distribution of Internet Protocol Addresses and Autonomous System Numbers, the IETF evaded much of the attention that would be associated with an attribution of regulator of the Internet. But I suspect that the level of desperation in such a search is growing in line with the levels of abuse, centralisation and dependence that we are seeing in today's Internet. No organisation with a role in the orchestration of aspects of the Internet, including the IETF, can hide from such misattribution. Because to say that no one is in charge, and we've managed to do all this to ourselves in a totally random and unorganised manner, is just completely unbelievable!

Disclaimer

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

Author

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

www.potaroo.net