Evolving a New Internet Governance Paradigm

PRABIR PURKAYASTHA, RISHAB BAILEY

The Edward Snowden revelations on pervasive and dragnet surveillance over the internet by the US National Security Agency (and other allied security agencies) – coupled with the nature of control the US exerts over the internet and telecommunications the world over – make it imperative that there is a new international framework to govern the internet.

Prabir Purkayastha (*prabirp@gmail.com*) and Rishab Bailey (*rishab.bailey@gmail.com*) are associated with the Knowledge Commons collective, New Delhi.

This article examines the present state of the internet – its governance structures, economics and architecture – in light of the US security contractor Edward Snowden's revelations that lay bare the extent to which the US controls the internet and its ecosystem. Given that the internet now forms an essential part of the world's communications and commercial infrastructure, there is an urgent need to formulate a binding international framework to delineate rights and obligations inter se states as well as between states and individuals in order to ensure that the internet is used as a tool to promote peaceful exchange of information for the progress of humankind.

Cyber Security and Privacy

The Snowden revelations[1] make clear that the US government and its allies have been systematically spying on the whole world. This surveillance (carried out through intelligence organisations such as the American National Security Agency – NSA and the British Government Communication Headquarters – GCHQ) is all pervasive – voice calls, emails, secure networks and servers have all been monitored or broken into – and covers all countries including even close allies of the US (France, Mexico, Germany among others). Not only are all voice calls and emails monitored on a real time basis, but this data is also stored for future use.[2]

The actions of the US government and its allies pose a serious threat to the privacy of people, the security of countries as well as to their commercial interests. For instance, in the case of Brazil, the NSA accessed data in secure servers of the department of mines that is commercially important for US companies who are likely to bid for some of the oil/gas blocks of Petrobras.[3]

In the post-second world war period, the US formed the Five-Eyes alliance with the UK, Canada, Australia and New Zealand (formally called the UKUSA Agreement) as its partners, the key partner being GCHQ of the UK. Its major activity was that of listening to all global communications through its Echelon programme.

The NSA and its partners have hacked into the global communications networks at different levels. The first is the global telecommunications network. This has been greatly facilitated by the US being the major hub of the global fibre-optic network, followed by the UK, where a major part of the trans-Atlantic cables land.[4] The US has used its position as a global hub to force various fibre-optic network operators to give them physical access to their networks in lieu of landing rights.[5] The AT&T Folsom Street case made public how AT&T was giving NSA access to its cable network.[6] This access has now been replicated for other network operators who have landing stations in the US through specific agreements.[7] As more than 80% of global voice and internet traffic pass through the US, automatically, the US has access to all this traffic.[8] In addition, as the Snowden slides show, the US has also tapped into global submarine cables.[9] It was known that through the Echelon programme, NSA and GCHQ had tapped into the global satellite and microwave communications networks. It is here that the Five-Eyes alliance is useful – it provides global listening posts for such tapping.

It is now known from the Brazilian expose that US telecom companies have been used to break into Brazilian and South America's telecom networks.[10] It is now known but can be surmised that the Brazilian network is not the only one that US telecom companies have helped the NSA breach.

The NSA's access to this global data stream has been enormously strengthened by its close links with the US-based giant internet companies. US companies enjoy monopolies in various spheres of the internet economy (McChesney 2013). The levels of monopolisation in the internet space allow gathering of global citizens data on an unprecedented level.[11] This cloud data is subject to the US laws that enable surveillance over global

citizens.[12] As we now know, the US-based internet majors such as Google, Microsoft, Yahoo, Facebook and others have partnered with the NSA in various ways.[13] Whether they have been active partners or have been coerced under the US domestic laws is a moot point for rest of the world. While the specific access being provided by the internet majors have been a matter of dispute, there is no doubt that all these companies provide access to their data to NSA in real time (and enable storage for future data mining). Such real time access includes information such as who is searching for what or browsing what sites from where.

The third layer of access that the NSA has is through the US companies' dominant position as proprietary hardware and software vendors. Though the position of the US as the leading hardware supplier has been weakened in recent years, much of the network equipment – switches, routers, etc – are manufactured or designed in the US. It is possible to provide back doors in such equipment which only the company that has created the design or manufactured the hardware would know. This has been the US argument to NSA against using Chinese manufactured equipment, but the same agreement also applies to all US designed or manufactured equipment. Similarly, software can have back doors. The major software suppliers in the world are again US companies, therefore their working closely with NSA means the possibility of such back doors. Microsoft, for instance, has built such back doors into their software.[14]

Cyber security is not limited to surveillance alone. As the attack on Iran centrifuges in Bushehr showed, it can result in physical damages to plant and equipment. Such attacks can take down a country's grid, water and sewage systems, cause flooding by opening dam gates and even set in motion a Bhopal or Fukushima like disaster. One of the most significant aspects of the Snowden disclosures which has not attracted adequate attention[15] are the cyber attack targets that Obama has authorised – Presidential Policy Directive 20.[16] Such a directive implies that foreign networks have been penetrated[17] and their security systems already compromised; vital infrastructure of other countries have been pre-targeted and waits only a command to trigger a cyber attack.[18] The US has blocked all attempts to initiate a cyber war treaty arguing that such a treaty is not enforceable while going ahead with its cyber war preparations. This radically increases the risk of triggering an arms race in cyberspace and fracturing the internet.

Economics of the Internet

The internet economy is monopolised by global corporations based mostly in the US. This is for a variety of reasons including historical development of the internet, first mover advantage, etc, and also the ecosystem of the internet largely run by US companies. The levels of monopolisation of the internet ecosystem are unprecedented and monopolisation seems to have occurred across different platforms.

For instance:

(a) Cloud services: Out of the top 10 cloud services in the world today, nine are US-based with the odd one out based in Germany; four are non-US-based out of the top 30, with only one in a global South country – Dimension Data, South Africa.[19] In terms of revenues, in the second quarter of 2013, global infrastructure-as-a-service and platform-as-a-service revenues – or cloud services – accounted for some $2.25 bn in revenue, with Amazon taking a 28% of all market share (followed by Microsoft, Google, and IBM).[20]

(b) Search engines: Google enjoyed a global market share of over 80% in May 2013[21] and has had a share of over 60% of all global searches done since 2007.[22] The highest market share for a company based in the global South was Baidu at less than 1% of the market.

(c) Social media: Facebook had a global market share of 72.4% in March 2013.[23]

(d) Voice over Internet Protocol (VOIP): in internet telephony, Skype enjoyed a market share of 82% in 2011.[24]

(e) Amongst the major internet portals, Google accounted for about 44% of the global internet advertisement revenue in 2010 (Microsoft at 4%, Yahoo at 8%, Facebook at 3%).[25]

Similar monopolies can also be seen in the browser market, the e-reader and e-book market, as also in the case of domain name ownership.

The Internet Corporation for Assigned Names and Numbers (ICANN) controls the global domain name system and has recognised 17 domain name registrars for top-level domain names.[26] All the most common top-level domains (TLDs) are controlled by first world institutions with .com & .net operated by VeriSign, biz operated by NeuStar (both US-based companies), .info operated by Affilias (headquartered in Ireland), .org operated by Public Interest Registry (a US based not for profit organisation).[27] The terms of the services provided both by these organisations as well those of the regional (sub) registrars are mandated through contracts signed with the ICANN.

This real estate in cyberspace has significant economic value and most of it is controlled by domain registrars located in the US. Most of the high-level domains are also under US legal jurisdiction, as a consequence of the domain registrars being in the US.

This level of monopolisation of governance systems, eyeballs, as well as advertisement revenue gives these few internet giants massive power at the global level – both to shape the global narrative/discourse (as they become the dominant sources for global information exchange) as well as to further entrench their already dominant positions and global power.

Monopoly of the information and media space at the global level is clearly problematic due to its anti-democratic tendencies. As more and more media companies shift to the internet – print as well as television with IPTV, the advertisement revenue that sustains the media would tend to shift to global internet companies. The diversity of information and different standpoints, both of which are essential for global democracy would weaken considerably.

The high levels of monopoly also enable imposition of IP policies and practices (such as the use of Digital Rights Management) that are not in the interests of the global South.

The dominance of the internet economy also enables control over actual economic

transactions. In the Wikileaks case, the US government could lean on websites such as Paypal and others to starve it of its sources of funding.

Another issue of importance is that of taxation on internet-based activities and therefore tax revenues. In e-commerce transactions, while the income is generated in the country where the buyer resides, the taxes are largely paid where the seller resides. For instance, Amazon pays taxes in the US on e-books sold across the world, and as e-books can avoid traditional customs duties for import of books – both lead to revenue losses to the country where taxes would traditionally have been payable. The growth of global e-commerce is therefore a big threat to the tax revenues of the global South.

Internet Infrastructure

The US control over the internet is exercised in a variety of ways – through control of the infrastructure on which the internet operates, through the dominance of US companies over the internet services and its ecosystem, as well as through a control of governance, oversight and standard-setting institutions. All of this combine to ensure the hegemony of the US over the internet.

For the internet to work seamlessly, domain names, and numerical web addresses and network identifiers need to be unique; the ability to assign them allows institutional power to be projected over the internet. Management of these critical internet resources is exercised by a US agency, the Internet Assigned Numbers Authority (IANA), under contract to the US Department of Commerce. The IANA contract is currently held by a California-based non-profit ICANN.[28] The primary contracts regarding the functioning of the IANA were signed in 2000 and subsequently renewed in 2003, 2006 and the latest in 2012 (up to 2019, subject to two renewals in 2017 and 2019).[29]

The US Department of Commerce has a veto on any decision of ICANN. Further, as part of this agreement, the most lucrative and common top-level domains – .com, .net., .org, etc – are with US entities, also ensuring US legal jurisdiction over all such domains.

The US Department of Commerce and ICANN also control the root servers that comprise an essential part of the addressing system on the internet (for instance, the US department of commerce must approve all changes to the root zone file requested by ICANN). Of the 13 top-level root name servers, 10 are based out of the US (with two in Europe and one in Japan).[30] As mentioned previously, the root zone file is at the apex of a hierarchical domain name system – thereby giving the US government unilateral control over an essential portion of the internet architecture.[31]

The technical standards and protocols that determine the way the internet operates are also under the de facto control of institutions that again are located and under the jurisdiction of the US. Moreover, the majority of technical standards, though set by individuals, are in reality set by organisations, again largely located in the US.

The Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB) within another non-profit corporation, the Internet Society (ISOC), develop technical standards for the Internet. While these organisations are global and largely voluntary in nature, the composition and funding of these organisations render them more responsive to US preferences than to users' demands.[32] The weakening of encryption standards by the NSA is a case in point.[33] Voluntary organisations such as World Wide Web Consortium (W3C) tend (by virtue of their composition and nature) to be dominated by global North-based corporate interests and institutions that have the resources to participate in the standard-setting processes.[34] For example, recently, under pressure from the US media companies, W3C has accepted to discuss introducing DRM in HTML5 standards.[35]

Global Internet Governance

In more specific terms, there are four areas in internet governance that are of concern: cyber security, intellectual property, content regulation and the control of critical internet resources (domain names and IP addresses). On each of these, countries react differently based on how they perceive their national interest. While the US has been arguing for content on internet to be free from censorship by states, it wants all content that violates the intellectual property of US companies to be stopped and has even seized hundreds of such domains.

The view of the US and a number of those propagating an internet independent of nation states (or any form of multilateral control) is that the internet is and should be governed by contracts amongst parties and organisations and run under a multi-stakeholder model. This is the so-called bottom-up approach to internet governance. Much of the technical standards and protocols have indeed evolved in this way. However, this does not do away with the concept of jurisdiction over the internet, as companies, other entities and individuals operate under legal jurisdiction of various countries and are therefore answerable to laws of countries and regulatory agencies.

There are two problems with contract-based internet governance. One is that it has led to privatisation and corporatisation of the internet. The other is that contracts do not and cannot incorporate "human rights" or "sovereign rights" – the rights of either individuals or of nations. A bottoms-up internet governance, as distinct from developing technical standards and protocols, has no legal mechanism to enforce rights of people, corporations or sovereign rights of countries. Rights stem from either a country's laws or international treaties. By keeping the internet governance either under US laws or under "contracts", the US has ensured that there is no effective global body that can address NSA's invasive surveillance over other governments and people, and penetration of vital infrastructure of other countries. Neither is there any place for regulatory principles to be exercised – for example, progressive taxation policies for e-commerce transactions that would help developing countries.

The International Telecom Union that has jurisdiction over the telecom infrastructure and has tried to raise issues such as cyber security, has been stopped by the US and other developed countries.[36] The World Summit on the Information

Society (WSIS) 2005 had identified the need for enhancing other governments' role in internet governance, as can be seen from the Articles 68 and 69 in the Tunis Agenda.[37] This has yet to be addressed. The Internet Governance Forum (IGF) that was set up after Tunis is a body which can only discuss various issues but take no binding measures.

How can infrastructure required by every country – for communications and commerce – operate under a contract from one particular government? Granted, as a pioneer, the US deserves credit; but that cannot be an argument for control over a vital piece of global infrastructure in perpetuity.

Though the WSIS had identified the need for enhanced cooperation or a more participatory structure for other governments, no such structure had materialised. It is obvious that setting up such a body would require a global treaty explicitly setting up such a structure and giving it specific jurisdiction and powers. Alternatively, ITU remains the only other global body which can address these issues.

It is in this context that Brazil initiated a process within IBSA (India, Brazil, South Africa) for a different form of internet governance. It started with an IBSA workshop and culminated with a Declaration in Tshwane, South Africa in October 2011 for a multilateral, democratic and transparent internet. It focused on the "urgent need to operationalise the process of 'Enhanced Cooperation' mandated by the Tunis Agenda" of WSIS and endorsed the recommendations of the IBSA Workshop on Global Internet Governance, Rio de Janeiro held on 1-2 September 2011. These recommendations included a multilateral body under the United Nations (UN) for internet governance, policies, standard setting, dispute settlement, address developmental issues, etc. In short, the new body would fuse the prerogatives of the IGF, ICANN, etc, enhancing them under an intergovernmental frame.[38]

India thereafter (at the 66th meeting of the UN General Assembly on 26 October 2011) proposed the setting up of a new UN-based body – to be known as the UN Committee for Internet Related Policies (UN-CIRP) – to act as a nodal governance agency of the internet, under the broader umbrella of the UN. The committee was to comprise 50 member states chosen on the basis of equitable geographic representation and to work on the basis of advisory groups comprising all relevant stakeholders.[39]

Call for Multilateral Governance

Post the Snowden revelations, a number of the organisations connected to internet governance – such as ICANN, IETF, IAB, the W3C, ISOC and the five regional internet address registries – met in Uruguay on 7 October 2013 and issued a statement distancing themselves from the US government and its actions.[40] The statement "expressed strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance" and "called for accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing". While this is indeed welcome, the issue still remains that unless such a globalisation of internet governance takes place under a treaty-based framework, the rights of people or of countries cannot be protected. Therefore IBSA's call for a multilateral internet governance framework that can incorporate institutions such as ICANN, IANA, IETF, etc, appears to be the way forward.

Under the WSIS resolution, ITU has been given specific responsibilities regarding the internet. However, the US and its allies have fought to keep internet completely out of the purview of ITU. In the World Conference on International Telecommunications (WCIT) held in 2012, Dubai, the US and a number of countries refused to recognise that ITU could discuss any aspect of internet governance and walked out without signing the new International Telecommunication Regulations.[41] If the US and other developed countries oppose such a multilateral framework, developing countries should then have no other option but to move to the ITU for global internet governance. The ITU charter already covers data communications and therefore ITU has always been a body that could conceivably be the UN arm for internet governance. As a minimum, the ITU should take up expeditiously the issue of cyber security and use of cyber weapons that pose serious threat to the security of countries.

While it is important that there should be a global treaty under which internet governance takes place, such a body must incorporate certain basic principles to be followed by all countries. These principles should include as a minimum (and in no particular order) the following:

(1) Demilitarisation of the internet: This is crucial towards ensuring that the internet is used for productive purposes rather than an instrument of warfare. It is essential that the internet be used only for peaceful purposes and it is necessary that this be recognised by states in a binding and enforceable instrument.

(2) No unilateral disconnection or denial of service to a country/region: Every country, every society must have the right to connect to the internet and use the same in accordance with applicable law. There must be no unilateral ability to disconnect a country or a region from the internet without appropriate global sanction. The internet must be recognised as a global public utility in a similar way to how telecommunication networks are traditionally treated.

(3) Respect for sovereign rights and determination of scope of applicability of

domestic laws/jurisdiction issues: This forms an essential and possibly the most contentious aspect of any proposed international treaty given the possible consequences such recognition of sovereign rights may have on the "monolithic" nature of the internet (it is argued there may be a Balkanisation or fragmentation of the internet) as well as human rights related issues such as free speech and censorship. However, it is essential for any enforceable rights framework that such issues be dealt with at the international level.

(4) Respect for human rights, in particular privacy and freedom of speech: While the specific contours of the extent to which a right to privacy should be exercised (permissible exceptions, etc) are matters that could be the subject of consensus, it is worth noting that the principle itself is established as a part of customary international law. Privacy rights are recognised by the constitutions of over 80 countries and numerous international instruments including the Universal Declaration of Human Rights (A 12) and the International Covenant on Civil and Political Rights – ICCPR (A 17). Further, global treaties such as the ICCPR already deal with the human right to free speech and its applicability and enforcement in a global context for example, through the recognition of permissible derogations. These could form the basis of any such protection for human rights in the context of the internet. It is essential to institute some form of international cooperation to ensure uniformity of minimum standards as well as to put in place an appropriate enforcement mechanism.

(5) Other issues such as access for all and recognition of access as a matter of right, non-interference with signals/packets during transit, net neutrality, transparency of governance mechanisms.

(6) Need to ensure peaceful dispute resolution.

Other Issues

Internet governance is not the only issue arising out of the NSA revelations. Hardware and software back doors have also been used to hack into network routers, switches and computers. The importance of using free and open source platforms ensure a higher level of protection as the code is freely accessible and can be studied. No such protection exists for proprietary software. Therefore there is a need to promote free and open-source software across the board as against proprietary software and platforms.

For hardware, new initiatives for open hardware are coming up which needs to be encouraged, especially with countries joining together to promote open hardware initiatives.

The other area where the global South should jointly create new initiatives is to promote cloud services that are located in the global South. This is imperative to break the US monopoly over the internet.

NOTES

1 The term is used broadly to refer to the series of revelations made by various news agencies around the world such as *The Guardian*, *The Washington Post* and *O'Globo* subsequent to Edward Snowden handing over secret American government documents concerning the surveillance related activities carried out by NSA and its global allies.

2 See documentation available at http://www.theguardian.com/world/the-nsa-files

3 See http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html, http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

4 See the Prism slides available at http://en.wikipedia.org/wiki/PRISM_(surveillance_program), map of global submarine cables system can be found at http://www.submarinecablemap.com

5 See http://publicintelligence.net/us-nsas/

6 https://www.eff.org/files/filenode/att/presskit/ATT_onepager.pdf

7 See http://publicintelligence.net/us-nsas/

8 See http://en.wikipedia.org/wiki/File:Prism_slide_2.jpg, http://www.telegeography.com/telecom-resources/map-gallery/global-voice-traffic-map-2010/

9 See http://en.wikipedia.org/wiki/File:Upstream-slide.jpg

10 http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934, http://www.zdnet.com/brazilian-government-tries-to-deal-with-nsa-spying-7000017771/, http://rt.com/news/rousseff-telecommunications-probe-companies-nsa-392/, http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying

11 http://en.wikipedia.org/wiki/File:Upstream-slide.jpg, http://en.wikipedia.org/wiki/File:PRISM_Collection_Details.jpg, http://en.wikipedia.org/wiki/File:Prism_slide_5.jpg

12 https://www.eff.org/deeplinks/2013/06/modern-foreign-surveillance-legal-perspective

13 http://en.wikipedia.org/wiki/File:PRISM_Collection_Details.jpg, http://en.wikipedia.org/wiki/File:Prism_slide_5.jpg

14 http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data, http://www.theregister.co.uk/2013/07/11/snowden_leak_shows_microsoft_added_outlookencryption_backdoor_for_feds/, http://rt.com/news/windows-8-nsa-germany-862/, http://www.techdirt.com/articles/20130711/11540623769/latest-leak-shows-microsoft-handed-nsa-fbi-unencrypted-access-to-outlook-skydrive-skype.shtml

15 http://www.reddit.com/r/IAmA/comments/1nisdy/were_glenn_greenwald_and_janine_gibson_of_the/

16 http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text

17 https://www.schneier.com/blog/archives/2013/06/us_offensive_cy.html

18 http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story_1.html

19 http://talkincloud.com/tc100

20 http://www.theregister.co.uk/2013/08/22/amazon_cloud_size_report/

21 http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0&qpcd=1700

22 http://searchengineland.com/google-worlds-most-popular-search-engine-148089

23 http://visual.ly/social-media-market-share-2013

24 http://www.mobiletrendsblog.com/Mobile-Trends_Report_H12011.html

25 http://zenithoptimedia.blogspot.in/2011/12/quadrennial-events-to-help-ad-market.html and http://searchenginewatch.com/article/ 2130985/Google-Now-Owns-44-of-Global-Advertising-Market

26 http://www.icann.org/registrar-reports/accredited-list.html

27 The only non-US based organisations appear to be in charge of the following TLDs: .cat (Catalunya based multi-stakeholder institution), .museum (International organisation in charge of museums) and .asia (not for profit corporation registered in Hong Kong).

28 http://mondediplo.com/2013/02/15internet

29 https://www.icann.org/en/about/agreements

30 http://www.root-servers.org, http://www.isoc.org/briefings/019/, http://en.wikipedia.org/wiki/DNS_root_zone

31 Jonathan Weinberg, ICANN and the Problem of Legitimacy, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1088&context=dlj

32 http://mondediplo.com/2013/02/15internet

33 http://epic.org/crypto/dss/new_nist_nsa_revelations.html, http://www.wired.com/threatlevel/2013/09/nsa-backdoor/all/

34 http://www.digitalnewsasia.com/insights/web-consortiums-failures-show-limits-of-self-regulation

35 https://www.eff.org/deeplinks/2013/10/lowering-your-standards

36 http://newsclick.in/international/wcit-–-why-us-and-its-allies-walked-out, http://www.eweek.com/cloud/wcit-treaty-talks-end-in-dubai-with-walkout-of-us-allies/

37 http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf, http://unctad.org/meetings/en/SessionalDocuments/a67d65_en.pdf

38 http://www.un.int/india/2010/IBSA%20STATEMENT.pdf

39 http://itforchange.net/sites/default/files/ITfC/india_un_cirp_proposal_20111026.pdf

40 http://en.wikipedia.org/wiki/Montevideo_Statement

41 http://www.itu.int/osg/wcit-12/highlights/signatories.html, http://www.thehindu.com/opinion/lead/a-false-consensus-is-broken/article4222688.ece, http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/

REFERENCE

Mc Chesney, Robert (2013): "The Digital Disconnect: How Capitalism Is Turning the Internet against Democracy".