Cross-Border Information Governance:
It's Time to be More Precise about Internet Governance

Brian E. Carpenter, December 2013

This note represents only my personal opinion. I was peripherally involved in the early days of the Internet governance debate some years ago, but I have only recently caught up on the discussion. To that extent, these are the contrarian views of an outsider.

Summary: 'Internet governance' is an ambiguous phrase that has led to confused thinking. There are serious societal issues that result from the existence of a pervasive data network, and these issues call for multi-stakeholder debate and governance. By contrast, there are mundane issues of technical coordination of Internet technology that function well today and need no new form of governance. The best way to avoid the present confusion of thought and argument is to use more precise language, to carefully distinguish technological from societal issues, and to focus on the societal issues individually. We should be discussing multi-stakeholder governance of cross-border information.

People are rightly concerned about various societal problems related to devices such as personal computers, tablets and smartphones connected to the Internet. The issues include

- consumer protection
- anti-competitive behaviour
- fraud
- software sabotage
- identity theft
- bullying & blackmail
- grooming
- undesirable content & misinformation
- on-line gambling
- intellectual property
- tax on cross-border transactions
- invasion of personal privacy
- unwanted surveillance.

These are all matters where legal and regulatory governance, as well as steps to educate and protect the public, are appropriate.

The phrase 'Internet Governance' was coined around 1995 and became widespread more recently, but it has a vague and contested meaning. Perhaps this is not surprising, because it was popularised in a highly contentious context, culminating in the Tunis session of the World Summit on the Information Society (WSIS) in 2005, an occasion at which many people met but their minds did not. The related Working Group on Internet Governance (WGIG) and the subsequent Internet Governance Forum (IGF) produced a lot of words, but essentially no action.

I suggest that the problem here is that the phrase 'Internet Governance' itself, although plausible at first sight, is too ambiguous to be useful. This has a consequence: any discussion purporting to be about Internet governance turns out to be inconclusive, because each participant has different expectations about the topic to be discussed and about the type of outcome that might result.

Let us first review the definition adopted by WSIS itself (recently characterised by Jorge Amodio as 'not universally accepted, and still under discussion how to interpret'):

> *Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*

The fundamental problem with this definition is that it is generic, so could mean almost anything to different people, yet it does not separate technological and societal issues. Also, it is quite unlike another commonly used and well understood phrase, 'corporate governance', which applies to a well-defined, finite body with a single management structure (such as a company), not to a diffuse construct like the Internet.

The definition does have one clear virtue, however: although it lists 'Governments' first, it does embed the multi-stakeholder approach in which governments are not preeminent. This is taken for granted in all that follows.

Technological issues – how data packets are formatted, how Internet nodes are named and addressed, how images and human-readable characters are encoded, how hypertext messages are constructed, and even which cryptographic algorithms are used, just to name a few items – need technical principles, standards, administration, and operational arrangements. To allow smooth network operations, these mundane matters need to be agreed on an open global basis, with a broad technical consensus among manufacturers, operators, and user groups. These are not matters for which the word 'governance' is helpful. An appropriate phrase is 'technical coordination'. This coordination has been in place since the 1980s. It spread long ago to be world-wide and it works well.

An example, which has become politicised due to certain apparent misunderstandings, is the administration of Internet Protocol (IP) numerical address space. For well-understood historical reasons, and as a contingent effect of the structure of the world economy, the supply of unused numerical IP addresses was already running out when the growth of the Internet started in developing countries. This was understood in the technical community by 1992 (a year before the World Wide Web was released) and the result was the definition of the extended IP version 6 (IPv6) address space by 1995. For those in a position to use IPv6, there has been no shortage of address space since then, and there will be no shortage in the technically foreseeable future (some say many decades; this author is prepared to say several centuries). IPv6 address administration is therefore a mundane matter, well coordinated by IANA[1] and the various address registries. The politicisation that has taken

[1] The Internet Assigned Numbers Authority (IANA) administers numerous technical parameters defined by the Internet Engineering Task Force (IETF) and others. It is currently an operational unit of the Internet Corporation for Assigned Names and Numbers (ICANN).

place is due to an apparent failure to appreciate the massive availability of IPv6 address space compared to legacy IPv4, and perhaps due to a false technical analogy with E.164 ('telephone') numbers, which have an intrinsically geographical allocation scheme.[2] IP addresses have no geographical connotation, so they do not need to be allocated geographically. This does not, of course, prevent them being allocated by national address registries, if a country finds it desirable to create one; but most countries manage very well using one of the regional Internet registries.

For clarity, this is independent of the need seen in most jurisdictions for traceability of IP address allocation, which we might describe as an audit requirement for address registries. This is indeed a matter for coordination between the relevant registry and local stakeholders.

The politicisation of the administration of the Domain Name System (DNS) also requires debunking. It has always been the case that Country Code domains are administered by (or on behalf of) the economy concerned, even for code designations that have an undoubted political aspect (such as *.uk* instead of *.gb*). In any case, the administrative decision to assign a new Country Code is not made by IANA. The administrative choice to create new generic Top Level Domains has economic implications (even, or especially, for new gTLDs that essentially fail due to lack of use). However, it is an *administrative* choice. Similarly, running the DNS root servers reliably, and securing the DNS infrastructure, are operational and technical chores. The same goes for enabling diverse character sets in DNS names. There is no governance magic in DNS names; they don't affect what content is or isn't available, where it is hosted, or which web sites are subject to surveillance.

Again, there is a likely need for traceability and audit of the domain names assigned to users. But that is nothing to do with the administration of TLDs or operation of the DNS service itself.

None of this implies that technical issues are without economic or societal effects. For example, the way international character sets are supported by the DNS may make certain types of fraud based on deceptive DNS names easier. The deployment of DNS Security will strengthen the traceability of domain names. In many cases, as mentioned above, IP address allocations also need to be traceable by the justice system. The way that the Border Gateway Protocol (BGP-4) operates has an impact on the economic relationships between Internet Service Providers. The availability of strong encryption has forced signals intelligence agencies to adopt indirect techniques such as metadata analysis instead of simple wiretapping. In these and other ways, technical decisions interact with society.

Avri Doria recently wrote that 'one person's technical coordination is governance to others' and this is undoubtedly true; the boundary is not hard and fast. However, the word 'governance' instantly attracts the attention of officials and politicians. It is my contention that the technical community has erred by using the word 'governance' too liberally to describe matters that are technical in nature, thereby creating a very real risk of official

[2] If the telephone system was invented today, E.164 would not need to be geographically based, but this was necessary in the past when telephone systems were electro-mechanical and international cables were rare.

intervention where it is not needed.[3] It has also confused the discussion about coordination with government where it definitely is needed. There do need to be points of contact between the technical community and those charged by society with, say, fraud prevention or criminal investigation. But this is coordination, not governance.

A corollary of this is that ICANN has little or nothing to do with governance. ICANN administers technical resources, in coordination with other technical organisations – an important job, but a different job from governance.[4] (ICANN itself needs good corporate governance, but that is another discussion entirely.)

Societal issues – what is considered appropriate or inappropriate use of the network, what counts as criminal use, what counts as invasion of privacy, what consumer protection is needed, economic impact, again just to name a few items – need societal principles, rules and so on. These are matters where, although there is considerable cross-border impact, we can expect every country to make its own rules. These are indeed matters of governance. But they are not governance *of the Internet.* They are governance of, say, pornography, child protection, fraud, personal or commercial privacy, truth in advertising, anti-trust law, etc. The primary resolution of these matters will mainly be national. Some matters certainly need to be discussed between many stakeholders; the issues cross borders when data cross borders, and so multi-stakeholder agreements will be needed.

A good example is the recent commotion in Britain about Web content filters. Their technical aspect is relatively unimportant. The transparent (unencrypted) nature of user requests to connect to a web site means that several techniques could be used to block requests for sites that are disliked by some people. Is this a good thing or a bad thing? This has nothing to do with Internet technology and everything to do with social attitudes and social constructs (political, religious or legal as the case may be). Whether it is good or bad for parents to be able to prevent children from getting certain information is a matter of opinion. The opinion may vary between families and between the members of each individual family. It will certainly vary between cultures and countries, and it will certainly vary across generations. It is not a technical matter. (See the public comments on the following web story for a variety of opinions: http://www.theregister.co.uk/2013/12/20/bt_lets_subscribers_turn_off_gay_education_sites/).

It's confusing, because the way in which societal issues arise has been changed by the use of the Internet. At one point in Western history, the argument was about whether the general population should be allowed to read the Bible for themselves. For more recent generations, the argument was about where dirty magazines or sex manuals were displayed in a shop. Today, the corresponding argument is about who controls the content filters. But it isn't the Internet in itself that needs governance, it's each individual issue. When we recognise this, and we remember that technological coordination isn't governance, we discover that, at its heart, the phrase 'Internet governance' is uninformative.

[3] The same applies to the word 'policy', for which I bear some of the blame, having used it when drafting the document that became the IETF-IANA memorandum of understanding published as RFC 2860.

[4] Here I disagree definitively with the WGIG report, which is explicit that 'names and addresses' are part of governance. WGIG unfortunately lumped technical administration in with governance.

A point that's often missed is that the societal problems we see are not a consequence of the specific technology of the Internet: spam is not caused by the details of the Simple Mail Transfer Protocol; surveillance is not caused by the details of the Internet Protocol or the Transmission Control Protocol; pornography is not caused by the details of the HyperText Transfer Protocol. The problems are intrinsic to any open data network enabled by cheap computing power and cheap telecommunications. They cannot be fixed by twiddling with protocols. As the Snowden revelations have shown, for example, surveillance is not prevented by encryption.

Of course, the technical community has work to do, to make the Internet as resistant as reasonably possible to known methods of misuse, but this is contingent upon current technology, whereas the societal issues are fundamental and unavoidable.

An analogy worth thinking about is with the road system. We have traffic regulations, many of which are virtually identical in every country, to directly protect lives and property on the roads. We have engineering standards to ensure that cars and roads are as safe as possible. But we don't consider that customs and immigration rules, laws against bank robbery, or laws about any other activity that may incidentally make use of the roads, constitute 'Road governance'. We have learned to clearly distinguish the road system from the uses society makes of it. We need to learn how to do this for the Internet.

At the moment, discussing 'Internet governance' has practically become a profession in itself. There is indeed a need for multi-stakeholder debate about cross-border information issues, but they should no longer be lumped together under a single phrase. Discuss 'cross-border surveillance' or 'cross-border fraud' or 'cross-border pornography' or whatever the *real* topic is. That might get somewhere. Discussing 'Internet governance' will continue to go nowhere fast. Worse, it will allow those who *really* don't want to discuss cross-border surveillance to obfuscate the issue. It also puts the Internet's highly successful technical coordination at risk of interference caused by confused thinking.

My personal suggestion to the IGF and to those upset by recent revelations about widespread surveillance, by cross-border fraud, etc., is simple: change the dialogue. Redefine the topic as 'cross-border information governance', unhook the debate from technological details, and focus on identifying the cross-border and multi-stakeholder consensus needed on each societal issue. The first step is to identify the specific societal issues and characterise the problems that they raise, without reference to specific technology. There is a preliminary list in the first paragraph of this document.

The Internet technical community has a part to play, but it is a secondary part and should not be driving the primary multi-stakeholder debate, which should be about society and information, not about technology. Nevertheless, the set of technological issues requiring coordination between the technical community and other stakeholders, including government bodies, should also be identified, and clearly labelled as 'technical coordination', quite separate from the societal issues that truly require governance.