Internet governance: what next ?

Abstract

Internet Governance has been the topic of endless discussion since the WSIS preparation was launched in 2001. Most States insist on having equal say in decisions bearing not only on technical matters, but also on public policy, and economic and societal matters, at both national and international level. However, the United States Government (USG) remains fully determined to retain unilateral control over the internet. While discussions may go on for any number of years, countries and citizens around the world cannot afford to remain sitting ducks unable to control their future. This paper explores possible actions they may take, without the USG approval, to protect their human rights and sovereignty, and to acquire some bargaining power in the internet realpolitik.

Keywords

monopoly, alternative, multiple-roots, RINA, internet-of-things

* * *
*

Internet Governance (IG) has been the topic of endless discussion since the WSIS (*UN World Summit on the Information Society*) preparation was launched in 2001. Most States insist on having equal say in decisions bearing not only on technical matters, but also on public policy, and economic and societal matters, at both national and international level. However, the United States Government (USG) remains fully determined to continue its spying and mass surveillance operations, and to retain unilateral control over the internet through a private Californian company, ICANN (*Internet Corporation for Assigned Names and Numbers*), created in 1998 for this specific purpose.

Rhetoric and wishful thinking may go on for any number of years, without any predictable outcome. While ideas and viewpoints may gradually become more flexible and negotiable, if the dominant party keeps expanding its power, there will come a time when negotiations will be irrelevant. Discussion with no possibility of counteraction is a losing game. Are citizens of all countries thus to remain sitting ducks waiting to be digitized and monetized? The ultimate goal of cyber-colonization.

What actions are possible ?

Unless it serves the interests of the USG, any action requiring USG agreement will be blocked. This is routine realpolitik. Hence, possible actions are those which can be implemented without the USG's approval, e.g.:

- apply national/regional laws to personal data privacy,
- apply national/regional fiscal laws to tax evasion,
- impose penalties on abusive market dominance,
- exclude illegitimate monopolies from major contracts,
- better balance investment/revenues between operators, content providers, ISPs and media,
- protect natural plants from illegitimate patents,
- create national/regional domain registries independent from ICANN,
- open competition between multiple DNS roots,
- use open source software,
- promote user friendly end-to-end email encryption,
- keep object identifier registries and standards under trade control (ISO),
- boost research/development on the future internet (RINA).
- . . others ?

To some readers this may look like a laundry list. However, in the context of standing up to a hyperpower a first level of defense is to make spying and predatory operations more costly. A second level is to carve out areas of independence to gain some bargaining power. In the longer term the objective is to make countries more resistant and better prepared for aggressive intrusions.

Many of these suggested actions are self-explanatory and need no further clarification. Let us look in more detail at the others.

• protect natural plants from illegitimate patents.

Example: an insect resistant indigenous pepper variety grows in a Least Developed Country (LDC). A multinational chemical group adds some useless ingredient to the seeds, and patents it. It then sues local farmers for allegedly growing the patented pepper without a license.

• create national/regional domain registries independent from ICANN.

Top Level Domains (TLD) such as .com, .net, .org, are familiar even to non internet users. Country code TLD (ccTLD) such as .cn, .de, .fr, .it, .us are also well known, while most people have never heard of e.g. .bz, .gl, .tp, .vi.

New TLDs presently being introduced such
as .bike, .construction, .guru, .photography, .singles, are largely unknown.

The USG imposed ICANN (created in 1998) as a monopoly in charge of all TLD registrations. This unilateral decision has no legitimate international basis. A good reason for such an anticompetitive status was to endow ICANN with a permanent cash cow fed with domain rental fees paid by internet users. In addition the costs of operating root name servers is by and large supported by State (sponsored) institutions and private companies that do not charge ICANN for this critical service. Such mostly hidden subsidies constitute unfair competition for independent roots and registries.

As usual with monopolies - and in this case backed by the USG - ICANN's top priority is making more money for its lavish life style and buying new friends. Being in the position of both TLD regulator and financial beneficiary is a blatant case of conflict of interest.

There is a dire need to put the ICANN house in order and subject it to competition from other actors in charge of defending user interests.

In fact, starting in 1996, before ICANN was set up, there were independent registries created, some were operated for several years, and a few are still in existence, e.g. Name-Space, Cesidianroot-Europe, OpenNic, Slash/dot, Name.coin, etc. An unknown number of private registries operate outside of conventional institutions and are mostly invisible. Whether due to ignorance, misinformation, or ICANN monopoly, independent registries are presently limited to niche markets. As no international legal instrument protects the ICANN monopoly the market could swing in other directions should States or large institutions change policies, or forego them.

• open competition between multiple DNS roots.

In the domain name field the term "**root**" designates a data set (usually a text file) containing a collection of TLD parameters. This file is duplicated within "name servers" queried by browsers and other applications to obtain an IP address associated with a TLD. In a nutshell this is the equivalent of looking up a subscriber's number in a phone

directory.

Root is a technical concept: it contains the TLD parameters. **Registry** is an organization managing domain users and their identifiers. A registry may use its own root (OpenNic), or the root of another organization (PIR, *Public Internet Registry*, uses the ICANN root).

The ICANN dogma is that what is needed is a single global (i.e. USG controlled) root. As mentioned earlier independent registries and multiple roots have been in operation for longer than ICANN, but they ill suit a monopolist empire. Curiously Google and OpenDNS, which are not registries, use their own root, copies of ICANN's.

The issue of a multiple root environment must be further explored in an article devoted to the subject.

• promote user friendly end-to-end email encryption.

After Edward Snowden's revelations it is no longer possible to view security with benign neglect. Many, but not all, organizations will try harder to integrate security in their procedures. This will be reinforced by commercial pressures from the security industry. Encryption is the basic ingredient of secure communications; it is used routinely in closed environments, but practically never in open environments. Email is by and large the dominant vessel for private and professional exchanges. As long as encryption is awkward to use or very slow it will not be adopted by the general public. In addition there must be a limited set of standardized protocols implemented in all mailers. At this point campaigns inciting users to adopt such safeguards could have a chance to succeed.

• keep object identifier registries and standards under trade control (ISO).

It has already been projected that the order of magnitude of objects in the internet will be 3 to 5 times larger than the number of humans. Tools will be necessary for registration, retrieval, and exchange of identifiers. Using DNS (*Domain Name System*) tools for handling this type of data seems inadequate and unrealistic. An example of a practical system is GS1 for bar codes and RFID. It is successful because it is carefully tailored to the needs of a specific trade: worldwide distribution of mass produced consumer goods typically available in supermarkets. Automobiles, chemicals, hospitals, wine, would have different needs. If the identifier management market falls into the hands of a world monopoly, it will impose its own proprietary standards irrespective of specific trade needs, and will distort manufacturing or distribution processes for its own profit.

Care must be taken to foster consensus within trades for identifier management standards anchored in a reputable international organization such as the ISO (*International Organization for Standardization*).

- **boost research/development on the future internet (RINA).**

As it stands today internet is an overpatched experimental system based on 40-year old concepts. The writing on the wall is "obsolescence". Research into the future internet has gained more interest over the past ten years, mainly through separate projects without any focus on specific operational targets. A team at Boston University managed to make a breakthrough in network design, published in "Patterns in Network Architecture" by John Day. The system name is RINA (*Recursive InterNetwork Architecture*). European teams received contracts from the EU Commission research programme to expand the initial platform by developing applications. This is an opportunity for a new generation of designers to close the security gaps of the legacy internet.

Trust is gone.

This is a matter of fact, even though trust is subjective. "If you want peace, prepare war" is a well-worn mantra. We don't really know how people in the USA will react to mass surveillance, for decades supposed to exist only in countries like China, Russia, East Germany, and so many others. The logistics has reached a point from which there may be no return. A totalitarian regime more Orwellian than ever might take over. We must convince our governments and fellow citizens to steer clear of that model and technology. We don't want to live in that kind of society, do we ?

Louis <Pouzin@eurolinc.eu>
v2.3 February 2014