Network Surveillance and the Snowden Watershed[1]

Carlos A. Afonso

October 2013

In his interesting text, Bruce Schneier[2] compares the different leverages individuals, groups, corporations and governments have over the Internet as it evolved, and its consequences for political action and control, using a sort of isomorphic comparison with a feudal society. One crucial aspect of this leverage is something which has been the practice of several countries' governments, following on the steps of the United States, for decades: surveillance in the name of national security.

Suddenly, with the Snowden watershed, this has become a ubiquitous reason for concern -- people and governments seem to discover that there is pervasive surveillance using telecommunications and Internet networks, and that not only the metadata of anything we (citizens and institutions of any country, anywhere) do on the Internet, but also the very content of our transactions (be it a video streaming, a voIP call, an e-commerce transaction or just a post or a visit to a social network service) are being monitored and peeked into.

Even more, this systematic collection of information is done under contract between intelligence agencies and telecommunications operators, as well large Internet application providers, with such pervasiveness which makes the 2006 NSA-AT&T network wiretapping event reported by the EFF a little more than a drop in the ocean.

Governments in many nations have become major users of the Internet for a variety of public services. Estonia is a good example of this use to enable e-government services. On the other hand, as rulers within their geopolitical borders, they are more and more wielding their regulatory, legislative or plain repressive leverage to impose controls and surveillance in the name of national security.

The recent NSA revelations are opportunistically being used by governments to propose rulings which amount to nothing less than surveillance allegedly to protect their people from surveillance. In the wake of those revelations some high-ranking Brazilian officials are proposing that the telecommunications regulator (Anatel) literally takes over the governance of the country's logical Internet infrastructure, and the agency is already issuing specific rulings accordingly. Brazilian subsidiaries of the five transnational telecommunications companies which control the main backbones in the country are even asking the government to hand over to Anatel the assignment of ".br" domain names and IP addresses.

Since 2011 these government sectors in alliance with the telecommunications oligopoly are striving to cancel a government ruling from 1995 (Norm number 4) which established the Internet as a value-added service beyond the purview of the telecommunications laws and regulations. This would simply amount to blowing the entire historical process of building and consolidating a pluralist system of Internet governance, which is widely regarded internationally as an exceptional achievement, to oblivion. Indeed, the Brazilian Internet Steering Committee (CGI.br), if these sectors have their way, would be reduced to an advisory commission or just be disbanded by decree.

[1] Published in *Mind*, #6, Berlin-Bali: October 2013, pp.37-38.

[2] Bruce Schneier, “Power in the Age of the Feudal Internet”, *Mind*, op.cit., pp.16-20.

At the same time, leading economies have developed advanced worldwide parallel networks, with gateways to the Internet, to run "protected" services. As one example, estimates show that in the wake of the US military's increasing reliance on remote-controlled vehicles ("drones") for running its wars on a planetary scale, about 40 countries are doing the same, and these systems run in protected networks also using the same data connection and transport technologies as the Internet's. Similar parallel networks are deployed for a variety of wiretapping functions.

As professor Milton Müller has stated in a 2012 article, "[t]he biggest threats to Internet freedom today do not come from intergovernmental organizations. They come from national governments with the institutional mechanisms to regulate, restrict, surveil, censor and license Internet suppliers and users."[3]

In the same article Müller also states that "it was the Internet - the ability to network computers across borders, free from nation-state controls and permissions - that opened up this new world [of global communications] for us." Yes, the Internet opened up a new world of communication and integration, but it did not penetrate geopolitical borders without having to overcome diverse governmental hurdles. In several countries significant pro-Internet lobbying and advocacy was necessary to circumvent legal and regulatory barriers, in several cases confronting state telecommunications monopolies, imposing of absurd taxes on users' or networking equipment, or simply prohibiting the new network to be established even for academic purposes.

In Brazil the very TCP/IP protocol was illegal (by rule the state telecommunications monopoly allowed only for OSI/ISO standards) and remained formally so until the privatization process in the late 90's, although the first permanent international links of the Internet started to operate under the protection of a host country agreement with the UN for the UNCED 92 conference.

There is one aspect of the impressive achievements described by Estonian president Toomas Ilves[4] regarding the development of the Internet in Estonia which remains ellusive. Since his country joined NATO even before becoming a member of the European Union, and is a member of the OSCE, it would be interesting to know how it reconciles its exceptional cybersecurity and e-governance infrastructure with the protection of its own people against the pervasive invasion of privacy practiced by government agencies, in particular the National Security Agency of the United States.

[3] *https://www.sfgate.com/opinion/article/Greatest-threat-to-Internet-governments-3723621.php#page-1*

[4] Toomas Hendrik Ilves, “Cybersecurity: A View from the Front”, *Mind*, op.cit., pp.14-15.