Open season

Written by: Geoff Huston, Chief Scientist, APNIC*

© David Rooney

I'm sure you've all heard about "the open Internet." The expression builds upon a rich pedigree of the term "open" in various contexts. It gives the impression that "open" is some positive attribute, and when we use the expression of the "open Internet" it seems that we're lauding it in some way. But are we, and if so, in what way?

A useful characterisation of "open" is the Internet's use of free, publicly available standards that anyone can access and build on to. This represents a major shift from the world of closed vendor-specific technology standards of just a few decades ago, as was common, for example, in the realm of mainframe computer technology. These days, new providers can introduce goods and services that they can confidently expect to be fully compatible with the existing Internet infrastructure. Under this principle the Internet is not closed to new investments in the provision of good and services, and it minimises the barriers to entry.

Another useful characterisation is that the Internet is "open" to all forms of traffic, and will treat all traffic that flows across the network in roughly the same way. This principle of the Open Internet is sometimes referred to as "net neutrality." Under this principle, consumers can make their own choices about what applications and services to use and are free to decide what lawful content they want to access, create, or share with others. This openness promotes competition and enables investment and innovation.

The Open Internet also makes it easy for anyone, anywhere to launch innovative applications and services, changing the way people communicate, participate, create, and do business. If you develop an innovative new tool that allows communication, you don't have to obtain permission to share it with the world.

At the same time, this openness is extremely fragile, and has very definite limitations that dampen this somewhat utopian ideal. The underlying technology may be freely accessible, but that is not the same as freely usable. The Internet is built upon a towering structure of smart, intelligent, efforts, which means it is by no means free of Intellectual Property Rights. Nor are the underlying network transmission and switching resources infinite, so when the aggregate sum of demand for access exceeds available capacity, then a service provider may choose to implement selective degradation of the services in order to preserve the integrity of the most essential traffic or protect the most lucrative revenue sources. Increasingly, we are shutting down the areas of potential innovation in communication models in order to concentrate our efforts to support a small number of service models.

These days the means of communication on the Internet are limited to a conventional "client/server" transactional model, and it's limited to a behaviour that sits upon a web transaction. Many other forms of interaction, such as peer-to-peer services, are often blocked by various forms of accreted network middleware. Perhaps the largest problem for open innovation in today's Internet is the Internet's own success and ubiquity. The incumbent providers can access economies of scale of operation that are inaccessible to all others, which allow them to gain positions of market dominance, and the stasis of the installed base means most forms of novel innovation fail to gain the threshold critical mass of acceptance needed to ensure a future. The larger the installed base the higher this threshold of acceptance of innovation becomes. Tensions are also apparent in the area of privacy and security. Should an open Internet support a user's choice to use tools, services and devices that preserve the user's personal privacy to the maximal capability of today's technology? Or should the considerations of security of the broader society place limits on the extent to which individual actions can be completely and totally concealed? Should we tolerate an increasingly toxic open network that exposes all of us to various forms of attack and exploitation? How can we ensure that the millions of devices that people,

businesses and public authorities connect to the Internet cannot be subverted and readily transformed into a catastrophic attack vector?

None of these questions has a clear answer. But they are pressing questions for public policy. Behind a dazzling veneer of high technology, the Internet is still just another form of the public communications space, and whether the Internet's various investment vehicles use private or public capital, the space in which we work and play on the Internet is always a public space. This means that while market forces strongly influence the day-to-day conversations about the Internet, the longer term debate needs the presence of a strong public voice to defend societal values. It is incumbent on us all to ensure that the open Internet continues to serve all of us, preserving essential qualities of ubiquity, accessibility, safety and utility that we should expect from every public common space.

As an international public organisation in pursuit of "better policies for better lives", the OECD must now add its perspective to the continuing discussion about what it means to be responsibly "open" on the Internet.

*APNIC is Asia Pacific Network Information Centre, see www.apnic.net