BoR PC12 (22) 17

A Standardized Internet Eco-System between European Union and Australia

Part 1

By

Syamantak Saha

Founder of Zapaat Internet Search Engine

30/07/2022

Table of Contents

I. Introduction

BEREC is the designated body for the European Union to regulate Electronic Communication, a large part of which is the formed Internet. A formed Internet operates within the European Union, with which users within the EU, undertake various activities of digital commerce including online shopping, banking, education and professional work. With an increase of trade activities between Australia and the European Union, there is a corresponding increase in online transactions that are occurring between Australia and the European Union that includes such online activities.

Businesses and end users are expecting a technically systemized and centrally regulated Internet platform where they could undertake their daily activities. Buyers in Australia and sellers in the European Union, and vice-versa, are expecting a stable set of technology that can be used to buy and sell goods and services reliably between Australia and the European Union.

II. Current Challenges

Whilst the Internet has achieved a high level of uptake in contemporary economies, however it has not been without its associated challenges. The particular challenges that are faced by businesses and end-users of the Internet for online commerce are :

a. Chasing Technology

Whilst Internet technologies and protocols are developed and advanced on a daily basis, for an economic utilization of a developing technology, the associated engineering underlying the innovation has to be stable, developed and propagated so that businesses can build a secure business model with it. End uses of online customers can also develop a method to connect, order and secure procurement based on the stability and security of the underlying technologies.

However, this simple model for business stability is heavily challenged with continuous and daily development of Internet technologies that de-stablize any underlying engineering for successful digital commerce. The situation is almost alike an engineered Bridge across a river that is changing in structure, lanes and speed limit everyday that commuters who have to travel across the bridge on a daily basis are finding it difficult to plan and undertake their business due to such economic uncertainty.

This Chasing Technology phenomenon, causes a dislike and de-preferencing of online activities for both businesses and end-users, as a IT Project could be undertaken with several costs, however as soon as being implemented would incur a significant change in the underlying technology, making the online innovation useless as soon as it is produced. Gradually, businesses and customers move away from using online technologies and the Internet to undertake their economic activities and the contribution to the real economy, in terms of saved labour costs, energy efficiency and business profits become harmed by such outcomes. Indeed, business may loose their income because customers would not be willing to buy products and services online, and they are unable to physically travel to the outlet to make a purchase.

b. Cybersecurity Issues

Personal data protection has taken a center stage whilst regulating the Internet economy. As regulations are passed both in the European Union and Australia to protect personal data including particular online transactions, its technical feasiblity is constantly challenged by developing technology. A technical implementation of data privacy for online users maybe introduced by a business, however, a latest technology when used in conjunction, may over-ride such security implementations, causing the customer to loose their personal data to online hackers.

This is particularly visible when using websites that use online advertising. An online user may be visiting an authenticated website for their transaction, such as online banking or shopping, however such a website when using a third party software to display online advertisements, could result in the user loosing their online activities data often stored in cookies to this third party advertisement provider, that is then used to display interactive advertisement to the user immediately. In this case, whilst data privacy laws are passed and to be implemented, in technical terms, its implementation becomes a challenge when there is a cross section of the current business website with a third party provider, who maybe using a state of the technology that is later than the standard level of technology being adopted by the business.

Also, in terms of law enforcement, a third party business that does not operate within the jurisdiction of the consumer, could try to provide run-away technologies that either disguise or dissolve cybercrimes post execution and being in a different country or economic zone, are not completely under the risk of capture. Indeed, several such activities do not even require legalized currencies as operational revenue and are known to use Cryptocurrencies for their transactions, a reason why cryptocurrencies appreciate extremely in value and are gradually being made un-lawful in the economically regulated territories.

c. Heterogeneous Internet Networks

An essential element of the Internet is to have a secure Client to Server connections for a safe and reliable TCP/IP and HTTP connections. When a data packet travels from the Server to the Client, technologically it assumes a uniform network during the transmission session. If a data packet travels from the Server to the Client over a heterogeneous network, meaning where the network capacity is different, it could cause eventual data loss and re-transmission. For example, if the Server is hosted in a network that has 100 Megabytes per Second transmission capacity, and there is an interim network of 20 Megabytes per Second and then the final Client on a network of 10 Megabytes per Second, there would be delays from transmission of data from the interim network to the Client, possibly causing a data loss during transmission and eventual re-transmissions. The technology used in TCP/IP including the 'Handshake' protocol with SYN/ACK data being timely received and acknowledged would cause a data error when used across considerably differentiated networks.

By increasing the SYN/ACK timeout sessions for packet transmissions, it would introduce the risk of cyber-attacks such as MITM and its variations, and so an associated network capacity of the Server should match that of the Client and should not ever be significantly different due to such reasons.

III. Recommendations

Initially, to have a successful Internet Ecosystem between Australia and the European Union, the above issues should be adequately mitigated. By doing so, both businesses and consumers would have a stable and secure Internet platform based on which they can then develop their business and maximize their individual economic outputs. It is recommended that the above issues be mitigated by certain adoptions as described.

a. Defining Internet Technology Options

To divulge the risk of Chasing Technology that may eventually leave businesses out of pocket and individuals at a risk of life, a certain standard for using Internet technology should be adopted. Australia and European Union should agree on a list of Internet Technologies and their associated features and versions that should be used for developing online solutions for business. This may include details of programming languages, specific features of each usable language and the most updated version of each such language that can be used. This is important because, a business may try and use a latest version of a programming language that may then cause a risk for the business and customers due to the underlying Internet network not having the capacity. Latest features of several programming languages use high-bandwidth internet connections to deliver services and a business adopting an online business solution may easily fail when attempting such projects, if not with adequately equipped Internet infrastructure.

b. Approving Foreign Third Party Online Providers

Whilst regulations exist to prevent the transmission and use of personal data without consent and for commercial purposes, third party service providers would still undertake such activities including stealing of personal information for their specific business purpose, defying law enforcement from foreign jurisdictions.

Australia and European Union should mutually develop a list of foreign operators who are allowed to provide electronic services to the connected economy, in order to prevent and protect the individuals personal data privacy and protection rights, and associated abuse that may currently occur in breach of such conditions.

c. Define Minimum Network Capacities

Australia and EU are large economies with sections of the population being provided varying levels of Internet network capacities. Regional areas in both economies have considerably lower network capacity that heavily populated and urbanized locations. In order to have equal access to the Internet for both communities, a minimum network capacity for the network should be defined and developed. Internet Service Providers would have to build and commit to this minimum network level of at least 3 Megabytes per Second download speed per connection for it to be legally considered an Internet connected economy. Businesses in Australia and the EU would then assume such uniform Internet network for developing their respective business solutions.