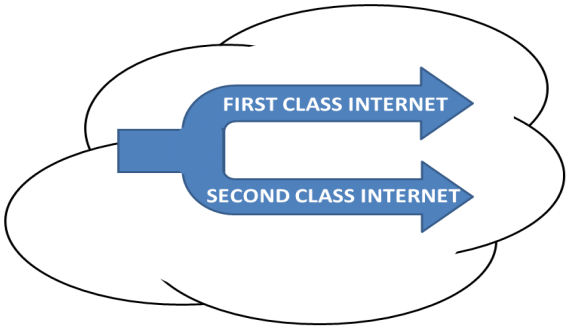
CDNs and Net Neutrality

www.adolforosas.com adolfomaria.rosasgomez@telefonica.com

June 2014



1. Introduction

In these weeks many articles appear that go in favor or against (very few) net neutrality. This 'net neutrality' topic has been present in legal, technological and business worlds for years but it is gaining momentum and now every word spoken by FCC or by any of the big players in this issue unleashes a storm of responses.

In this hyper-sensitive climate it may seem that anyone could have and show an opinion.

I've seen people that do not work in Internet, do not work for Internet and do not work by means of Internet and who do not have a background in technology, legal issues or social issues shout their opinion in many media. Defending net neutrality is popular today. It sounds like defending human rights.

The natural result of this over-excitement is that a lot of nonsense is being published.

How can we harness such a difficult topic and bring it back to reason?

In this article I will try to pose the 'net neutrality' discussion in right terms, or at least in reasonable terms, connected to the roles that Internet has reached in technology, society, economics and specific businesses as content businesses and CDNs which are specially affected by this discussion.

2. What do they mean with Net Neutrality?

The whole discussion starts with the very definition of Net Neutrality as there are many to choose from. The simpler the better: Net Neutrality is the policy by which we ensure that no net-user is 'treated differently' or 'treated worse' than other net-user for the sole reason of having a different identity.

I have selected a definition that on purpose avoids business terms and technology terms. This is a good starting point to dig in the meaning of 'net neutrality' and inquire for the massive response that it is rising.

What does it mean a 'policy' in 'net neutrality' definition? A policy is a consolidated behavior. It is a promise of future behavior. It is a continued and consistent practice.

Which is the 'net' in 'net neutrality' definition? It is Internet. This means every segment of network that talks IP to/from public IP addresses.

Who is the 'net-user' in 'net neutrality' definition? He is anyone linked to a public IP address. He is anyone that can send and receive IP packets through a public IP address.

What is 'treating someone differently' or 'treating someone worse than others' in 'net neutrality' definition? As we are talking about 'network-level behaviors', treating means dealing with network-level objects: packets, addresses, traffic… So we can translate that ambiguous 'treating worse' to: handle packets, handle addresses, handle traffic from someone differently/worse than we handle packets, addresses, traffic from any other just because we know who is the traffic originator.

How can we 'deal worse' with packets/traffic? There are some network-level-actions that affect traffic adversely and thus can be interpreted as 'bad treatment': delaying/dropping packets in router queues.

Why would ANYONE delay/drop packets from anyone else in a router queue? There is no reason to harm traffic flow in a router just for the sake of doing it or to bother someone. It is plain nonsense. But every minute of every day routers delay packets and drop packets…why? The reason is routers are limited and they can only deal with X packets/s. In case they receive more they forcefully need to ignore (drop) some. This fact should be no major drama as most transport protocols (TCP) deal with lost packets, and all end-to-end applications should deal with continuity of communication no matter which transports they use. The only effect that we can acknowledge from packet drops is that they create a 'resistance' to make packets through Internet that increases with network occupation, but this 'resistance' is statistically distributed across all net-users that have communications going through each router. No one sees a problem in that. It is the same condition of a crowded highway, it is crowded for the rich and for the poor…no discrimination. Classic routing algorithms do not discriminate individual IP addresses. They maximize network utilization.

3. Does (recent) technology threaten net neutrality?

Despite congestion problems in internet have been present from the beginning of this now famous network, some people have recently developed a tendency to think that router owners will decide to drop some specific net-user's packets all the time. Just to harm this user. But why complicate the operator's life so much? It is easier to let routers work in best effort mode, for instance with a policy of first-come first-serve. This is in fact the way most internet routers have behaved for years. Just consider that 'routing IP packets' is a network layer activity that involves only checking origin-IP addr, destination IP-addr and IP priority bits (optional). This is very scarce information, that just deals with the network level, without identifying applications or users, and even for those 'quick routing choices' the routing algorithms are complex enough and internet is big enough to have kept routers for years under line-rate speed (usually well under line-rate speed) even for the most expensive and more modern routers. 'Priority bits' were rarely used by the operators until recently, as creating a policy for priorities used to degrade badly the router performance. Only very recently technology is going over that barrier. Read on to know if we can go much further.

As technology evolves it is now possible (in the few recent years , maybe 5) to apply complex policies to routing engines so they can 'separate' traffic in 'classes' attending to multiple different criteria that go beyond the classic layer 3 info : (origin, destination, priority). With the advent of Line-rate DPI (Deep Packet Inspection) some routing and prioritization choices can be taken based on upper layers info: protocol on top of IP: FTP, HTTP, MAIL… (this information belongs to layers 4-7) , SW application originating packets (this info belongs to layer 7, and has been used to throttle P2P for instance), content transported (layer 7 info, has been used to block P2P downloads)…

So it is now (maybe in the last 5 years) that it is commercially possible to buy routers with something close to line-rate DPI and program them to create first class Internet passengers and second class Internet passengers attending to many weird criteria. It is possible, yes, no doubt… but is it happening? Does it make sense? Let's see.

4. What is an ISP and what is 'Internet Service'?

Internet Service Providers, taken one by one, do not own a significant portion of the Internet, nobody does. So how can anyone offer to you 'Internet Service'? Do you think that all of them (ISPs of the world) have a commercial alliance so any of them can sell to you the whole service in representation of all of them? No.

Then, what is Internet Service?

We could define IS as being close to a 'Carrier Service', that is: a point-to-point messaging service. This basic service takes a 'packet' from one entry point (a public IP address) and delivers this packet to other (public IP addr) point. That is all. Well, it is in fact usually much less than that. This 'point-to-point service' is not exactly what ISPs sell to us. In case both points lay in the ISP network then yes, ISP contract means end-to-end service inside that ISP 'portion of internet' (nothing very attractive for anyone to pay for), but what if the 'destination point' is out of the ISP?. Does our ISP promise to deliver our IP packet to any public IP? Nope. Here lies the difference with Carrier Services. Internet Service cannot be sold as an 'end-to-end' service. It is impossible to provide that service. It is physically impossible to reach the required number of bilateral agreements to have a reasonable confidence that an IP packet can be delivered to any valid IP address. Internet Service is an 'access service'. This means that you are being promised to do all reasonable effort to put your packet 'on the way' to destination IP, but they never promise you to deliver. What does mean 'all reasonable effort'? This is subject of much controversy, but usually national laws of fair trade force the ISP to behave 'correctly' with locally originated traffic and 'deliver' this traffic in good condition to any Internet exchange or any peering point with any other company. That is all. Is this good for you? Will this ensure your IP packet is delivered, or better, 'delivered in good time'? Nope. As internet exchanges and peering points may distract us from the focus of our discussion lets save these two concepts for a couple of paragraphs later. (See 6).

(NOTE: we will see later that Internet Service, not being end to end, is not currently under the legal denomination of 'Common Carrier', and that is extremely important for this discussion.)

The Internet service is essentially different from 'Carrier services' that you may be used to.

It is important to review classic Carrier services in search of resemblances & differences to Internet Service.

5. Classic Carrier Services

The paradigm of Carrier Services is 'snail mail' or traditional postal service. No company does own the whole postal resources across the world, but there is a tacit agreement between all of them to 'terminate each other's services'. Each postal company (usually owned by a government) deals internally with in-house messages, originated in its territory and addressed to its territory. When a message is addressed 'out of territory' the company at origin requests a fee from the sender that is usually proportional to the difficulty

(distance) to destination. At the destination there is another postal company. This worldwide postal transport is always a business of two companies. The biggest cost is moving the letter from country to country and there is no controversy: the postal company at the originating country takes the burden and cost of moving the letter to the destination territory. And this effort is pre-paid by sender. For the company living in the destination, doing the final step of distribution does not take more than dealing with a local message. Of course the letter must be correctly addressed. These two companies usually do not exchange money. They consider all other postal companies to be 'peers' as roughly the same effort (cost) is involved in sending letters 'out' of territory (a few letters but a high cost per letter) than the effort (cost) to distribute foreign letters 'in' (much more letters but at a low local cost per letter). Roughly each company will spend the same sending out than it may request from all the other companies to deliver their messages. So it is just more 'polite' to not receive payment for dealing with foreign origins and in response don't pay to send messages abroad. Notice also that the local postal company does not need to 'prepare' anything special to receive letters from out of the country. The same big central warehouse that is used to collect all local letters is used to receive letters from abroad. This has worked well for postal companies for hundreds of years and it still works. Of course if a country falls in the rare state that no local people send letters out and at the same time local inhabitants receive tons of letters from other countries, the local postal company would have big losses as they have cost but no income. Anyway these situations are scarce if at all possible and usually postal companies have been subsidized or owned by the local government so losses have been taken as a 'fact of life'. Important facts to remember about this service: the sender pays per message. The originator company bears the whole cost of moving messages to destination postal company. Each destination may have a different price. Each destination may have a different delivery time. Letters above a certain size and weight will have extra cost proportional to actual size and weight and also to distance to destination. Local companies do not create additional infrastructure to receive foreign messages. There are no termination costs.

Another more modern 'Carrier Service' is wired telephony. As in the postal service no company owns the whole telephony network. As in the postal service there exist local companies that take incoming calls from its territory and deliver the calls to its territory. When a call originates out of territory the caller must do special actions: he must add a prefix identifying the destination territory. In the destination country a local company has an explicit (not tacit) agreement with many other companies out there (not all) to terminate the incoming call. As in the postal service the termination business always involves exactly two companies and the highest cost is transporting the call to the 'doors' of the destination company. As in the postal service the caller (sender) pays for the extra cost. An important difference is that the caller usually pays at the end of the month for all the calls and not before. Again these telephony companies consider themselves as 'peers' but with some important differences: in this service it is required to build and pay for a physical connection from company to company. In the postal service the originator company was free to hire trains, plains, trucks, ships or whatever means to carry letters to the door of the local post company. The volume of letters may vary substantially and it does not mean big trouble for anyone except for the originator that must pay for all the transport means. The receiving infrastructure is exactly the same as for local letters and it is not changed in size or in function by foreign workload. In telephony the local company must allow the entrance of calls at a specific exchange station. Telephony works over switched circuits and this means that the originating company must extend its circuits to other companies in other countries and connect on-purpose through a switch in the other company circuits. This now has a cost (which is not minor by the way). More important: this cost depends on the forecasted capacity that this exchange must have: the estimated amount of simultaneous calls that may come from the foreign company. Now the infrastructure for local calls cannot be simply 'shared' with foreign calls. We need to add new switches that cannot be used by local

workload. Notice that every new company out there wanting access to my company circuits will require additional capacity from my switches. No telephony company will carry alone the cost of interconnection to other companies in other countries. Now 'balance' is important. If a telephony company A sends X simultaneous calls to company B and company B sends Y simultaneous calls to company A now it is very important to compare X to Y. In case they are similar: X~Y, 'business politeness' leads to no money being exchanged. In case A sends much more than B: X>>Y, B will charge for the extra cost of injecting A's calls in B's circuits. Remember that callers pay A, but B terminates calls and receives nothing for doing that. Important facts to remember about this service: caller pays per call (or per traffic). The originator company bears the cost of extending circuits to the 'door' (switch) of the destination company. Each destination may have a different price for calls. Cost will be proportional to call duration and distance to destination. Local companies MUST create (and pay for) specific infrastructure (switches) and MUST reserve capacity PER EACH foreign company. This infrastructure MUST be planned in advance to avoid congestion. Cost of infrastructure is proportional to expected traffic (expected incoming simultaneous calls). There are termination costs in case of unbalanced traffic between companies.

6. Internet Service compared to Carrier Services

The Internet Service is sometimes viewed as similar to telephony. At the end, in many cases telephony companies have picked up the responsibility (and the benefits) of providing Internet Service. But Internet Service is an access service not an end-to-end service. How is this service built and run? An ISP builds a segment of IP network. If there are public IP addresses inside and they are 'reachable' from other public IP addresses, now this segment is part of internet. For the ISP it is no big deal to move packets to and from its own machines, its own IP addresses. The small ISP just applies 'classic routing' inside its segment. (Apply classic routing means: all routers in this small network share a common view of this small network and they run well-known algorithms that can determine the best path or route crossing this network from machine 1 to machine 2 possibly jumping through several routers inside the network. These routers have a distributed implementation of a shortest path algorithm based on selecting the next hop in a regularly re-computed routing table. As the required capacity of the routers depends on the number of IP addresses managed and the number of routers inside this 'small' network, there is a limit in cost and performance to the size of a network that can apply classical routing.)

What is interesting is what happens when destination IP is out of the 'small network'. The new segment of internet does not have a clue about how to deliver to destination IP. That destination IP may be at the other end of the world and may belong to an ISP we have never heard of and of course we do not have business with them. The ISP does not feel bad about this. It is confident that 'It is connected to internet'. How? The ISP is connected to a bigger ISP through a private transit connection and the smaller ISP pays for transit (pays for all the traffic going to the bigger ISP), or it is connected to a similar ISP through a peering connection, or it is connected to many other ISPs at an internet exchange. Usually peering happens between companies (ISPs) that are balanced in traffic, so following the same reasoning that was applied to telephony they do not pay each other. Internet exchanges are places in which physical connection to others is facilitated but nothing is assumed about traffic balance. The Internet Exchange is 'the place' but the actual traffic exchange must be governed by agreements 1-to-1 and can be limited to keep it balanced as 'free peering' (no charge) or on the contrary it may be measured and paid for as a 'paid peering'.

We have said that smaller ISPs pay for transit. What is 'transit'? Small ISPs route packets inside their small network, but to connect to internet they must direct all outgoing traffic through a bigger ISP router. This bigger ISP will see all these IP addresses from the small ISP as their own addresses and apply classical routing to and from its own machines. The bigger ISP supports the whole cost of the transit router. For an ISP to accept traffic in transit from smaller ISPs the transit routers must be dimensioned accordingly to expected traffic. This big ISP may not be very big and so it may in turn direct traffic through transit to a bigger ISP… At the end of the chain, the biggest, worldwide ISPs are called 'tier 1'. These are owners of huge networks; they are all connected to all the rest of tier 1's. They see IP addresses of other tier 1's through 'peering points' in which they put powerful routers. The cost of the peering infrastructure is supported by both the two ISPs connecting there. They do not pay for traffic but they invest regularly in maintenance and capacity increases. It is of key importance to both peers to account for the traffic going through the peering point in both directions. They must maintain it balanced. If a misbalance occurs it is either corrected or the ISP that injects substantially more traffic will have to pay for the extra effort it is causing on the other side.

We have not yet demonstrated that the IP packet coming from the small ISP can find its way to destination IP. Let's say that destination IP belongs to a small ISP that is 20 'hops' (jumps) away from origin. In the middle there can be ten or more middle size ISPs that pay for transit to bigger ISPs and there maybe 3 tier 1 ISPs that peer to each other. The IP packet will be moved onto a higher rank network 'blindly' in its way up just for a single reason : all routers in the way notice that they do not know where lays the destination IP so their only possibility is to send the packet through the door (port) marked as 'way out into internet'. At some point in this way up the IP packet will reach a tier 1 network that talks BGP to other tier 1's. Some portion of the destination IP will match a big IP pool that all BGP speaking machines handle as a single AS (Autonomous System). Many tier 1's have one or more AS registered. Many ISPs that are not tier 1's also talk BGP and have registered one or more AS. What is important is that routers that talk BGP have a way of telling when an IP address is the responsibility of some AS. Let's say that in this case the first moment at which our destination IP is matched to a 'responsible destination network' happens at a tier 1 router talking BGP. This router knows one or more ways (routes) from itself to the destination AS so it simply sends the packet to the next hop (router) that best suites its needs. The next router does the same and in this way our IP packet traverses the tier 1 networks. At one of the tier 1's the destination IP address will be matched to a local sub-network; this means our packet can now be routed through classical routing algorithms. This classical routing will make our packet go down from bigger ISPs through transit routers to smaller ISPs until it reaches the destination machine.

What has happened in comparison to our good old carrier services? Now no one 'in the middle' knows what happened to the packet. They only know they treated this packet 'fairly'. Essentially transit ISPs just worry about the statistics about dropped packets in their transit routers and make sure that number of dropped packets is kept inside a reasonable margin. For instance 1 drop per 10^5 packets is not a drama for any transit router. But notice that a sudden change in a remote part of the world may increase this router losses to 1 in 10^3 drops and there is little that the router owner can do. In fact all he can do is to rely on global compensation mechanisms implemented at the highest routing level (BGP) that are supposed to slowly balance the load. But in the meantime lost packets are lost and they must be retransmitted if possible. In any case the application that is managing communication will suffer in one way or another. It is now impossible to plan for capacity end to end as routes traverse many companies and these companies are left to the only resource of measuring their bilateral agreements and react to what happens. The transit companies cannot know when traffic is going to increase as it may very well be that the originator of the traffic does not have contracts with any of them so this originator is not going to inform all companies in the middle of its capacity forecasts. Especially difficult is to realize that the dynamic nature of routing may cause

that sometimes this traffic causes effort to a certain set of companies and the next moment it causes effort to a different set of companies. For this reason Internet Service is NOT a Carrier Service, it does NOT carry a message 'end to end'. The IP protocol works end to end, but it is in practice impossible to establish the responsibilities and trade duties of the companies involved in the journey of a single packet. It is impossible to tell a customer of an ISP who (which companies) have taken part in carrying his packets to destination. It is impossible to tell him which is the average quality of the services that his packets have used to reach destination. Worse than all of this it is impossible to all the companies in the middle to prepare to give good service to all traffic that possibly will go at any time through their routers.

So in this terrible environment the companies carrying packets fall back to 'statistical good behavior'.

For this reason ISPs cannot charge their users for 'transactions' as they are not responsible for terminating a transaction nor they are able to set up a commercial agreement with one, or two or one hundred companies that could make them assume the responsibility of granting the transaction. So, as they do not charge per transaction they need a different business model to take traffic from net users. They have decided that the best model is to charge per traffic, considering traffic in a wide statistical sense. In the past and still in the mobile data today they charge per total amount of information sent over a period of time: GBytes/month. It is more common to charge for 'capacity available' at access not for 'capacity used' : Mbps up/down. This is a dirty trick and a fallacy in business as you may easily see: you are receiving an access service, your ISP wants to charge you 40$ a month for a 5/50 Mbps link no matter if you use it or not. But does this mean you can feed 5 Mbps to any destination IP in the Internet? Or do they grant you can receive 50 Mbps from any combination of other IP? Of course it does not. How could it be? Your ISP can at best move your 5 Mbps up to the next router in the hierarchy. But as you will see no ISP in the world will make a contract with you promising to do that. They will say they do not know how much of those 5 Mbps can go out up to internet.

I think it would be fair to force an ISP to measure incoming and outgoing throughput as an aggregate at the network edge. This means measuring all contributions in from: accesses + transit + peering, then measuring all contributions out to: accesses + transit + peering. Of course it is impossible to tell how many customers need to go 'out' at any moment so outgoing throughput may be sometimes a small fraction of incoming throughput. This ratio will probably vary wildly over time. The only number that should be forced as a quality measure onto the ISP is: the aggregate number of bytes taken from users at the edges of the network (from accesses + incoming transit + incoming peering) must equal the aggregate number of bytes delivered to network edges (out to accesses + out to transit + out to peering). If an ISP claims to provide 'Internet Service' it should be prepared to handle any situation, any possible distribution of incoming bytes to outgoing bytes.

Notice that it is cheaper if all bytes from local accesses go to other local accesses in the same ISP, in this case transit and peering are unused. Much more dramatic is the case in which all accesses suddenly need to send packets out through a transit router. This will not work in any ISP of the world. Packets will be lost massively at the transit routers. The usual business is to estimate the amount of outgoing traffic as a fraction of the local accesses traffic and then make transit contracts that grant ONLY that fraction of throughput out. These contracts are reviewed yearly, sometimes monthly but there is not much more flexibility. A sudden surge of traffic still can and often does cause bad experiences to users that coincide trying to make their packets through internet at the same time. This 'resistance' to go through is experienced in different ways by different applications : email will not suffer much, Voice over IP and Videoconference will be almost impossible and viewing movies can be affected seriously depending on buffering model and average bitrate.

You could hardly convince an ISP to over dimension transit contracts out. What happens if this ISP sees the transit unused for 12 months while still having to pay a tremendous amount of money for those expensive transit contracts? Naturally the ISP will soon reduce the contracts to the point in which the transit carries just the traffic the ISP is paying for. Unfortunately the interconnection machinery cannot be made flexible; it cannot be made to increase capacity as needed. For many reasons this is impossible. As you can see a cascading effect will be created if a few ISPs start over dimensioning their peering/transit machinery while keeping their contracts low… In case they need to flush a sudden surge of traffic the next ISP in the chain not having over dimensioned machinery will not be able to cope with the surge. Also notice that paying for a router that can handle 2X or 5X the traffic it actually has is very bad business and no one will do it.

Important facts to remember about this service: sender does NOT pay per message. He pays per 'max sending capacity installed at his premises'. The originator company does NOT bear the cost of extending circuits to the 'door' (switch) of the destination company. The originator company extends circuits JUST TO ANY other carrier in the middle. Interconnection machinery costs are supported by bigger carriers, not by smaller ones. Interconnection cost between equal sized carriers is shared between them. Each destination will have exactly the SAME price. Cost can NOT be proportional to distance to destination. Service is NOT an end to end transaction. Local companies MUST pay for using specific infrastructure (transit) to go out of territory; and they MUST build specific infrastructure and reserve capacity for EACH transit company that carries traffic into its territory. Both the outgoing contract and the inbound infrastructure MUST be planned in advance to avoid congestion. Cost of infrastructure is proportional to expected traffic (expected aggregated rate of packets/s). It is impossible to forecast the traffic of an incoming connection from a transit company as this company is a dynamic middle-man to an unknown number of traffic sources. There are transit costs in case of unbalanced traffic between companies; the small ISP pays the big ISP. Equal size ISPs do not charge each other for traffic they just 'peer'. There are infrastructure costs in every interconnection. Both 'peers' and transit providers spend lots of money buying and maintaining interconnection machinery.

7. Mapping 'net neutrality' to the crude reality of Internet access service

We have seen that Internet Service is an Access Service, not a Carrier Service. This fact is reflected in some legislation, particularly in the Anglo-Saxon world under the concept of 'Common Carrier Services'. These Services include but are not limited to postal service and wired telephony. These are services so important that usually have been admitted to be 'public interest service' and thus governments have interfered the market rules to make sure that these services were widely available, non-abusive, reliable, affordable, responsive… beyond the pure market dynamics.

So when we say 'do not treat IP packets differently in case they belong to different net users', how does this statement map to the Internet Service that we have described in the previous paragraph?

How can an ISP comply with the above definition of 'net neutrality'?

ISPs deal with packets; they have to route packets inside their network and also to the next middle-man in Internet. They get money from accesses (for availability) and charge/pay for Transit contracts (for available capacity and/or transferred traffic). Can they reconcile their business model with net neutrality? Yes, I do not see the problem. It is fairly simple. The flaw is in the business model. It is a very weak proposition to sell 'a reasonable effort to put your packets in its way to destination'. I'm sure people only buy this service because no other alternative is available. It is easy to drop packets at every interface when there is

congestion, possibly frustrating some users out there, and at the same time keep my promise of treating equally (bad) all net-users and at the same time maintain my business model based on 'reasonable effort'. Who decides what a reasonable effort is? Currently entities like FCC have a hard time trying to regulate Internet Service. As they cannot treat it as 'Common Carrier' it would not be fair to force ISPs to have a strict policy on transit contracts. How could they create this policy? Let's say that FCC forces every ISP to contract transit for a total amount of 10% of its upstream aggregated accesses…Is this enough? Who knows… It is Impossible to tell. Would this grant absence of congestion? No. Internet traffic varies wildly. You see the actions of the regulator will be very unfair for all ISPs and at the end they will not solve congestion.

8. CDNs… businesses beyond plain Internet Access

Now we have seen that plain Internet Service can be kept neutral due to the fact that 'access business model' is a weak commercial proposition essentially easy to accomplish to-the-letter while frustrating users.

Are there other Internet Services that cannot be reconciled with net neutrality? Do these other services (if any exist) distort the plain Internet Service? Is any ISP in the world abusing new technology to violate net neutrality, despite being easy to maintain strictly the neutrality claim? I will try to address all these interesting questions.

CDN: Content Delivery Networks, they are businesses that go beyond Internet Service. I'm sure you do not find strange that companies with an important message to communicate are NOT happy with a service that promises 'a reasonable effort to put your packets in its way to destination'. I will not be happy too. If I had the need and the money to pay for it I would buy something better.

CDNs are end to end services. CDNs are true carrier services. Very interestingly CDNs are not regulated as Common Carrier (not yet at least), but in my humble opinion they are as good carriers as any other end to end service. They sell transactions. They also sell traffic, but not bulk, best effort delivery, they impose SLAs to delivery. CDNs work to build special routing through known paths through internet, so they avoid the middle-man loss of responsibility. Once you know all the actors in the middle you can distribute responsibility and cost and you can make the service work with any quality parameter that you would like to set end to end.

Of course sending bytes through a CDN implies a loss of flexibility. Now routing cannot be the all-purpose dynamic routing of internet. You have to place machines of your own in the middle of the way from one end to another. You have to do many special agreements with network owners for collocation; you have to hire private links, install your own powerful routers, and install your own intermediate storages. All these actions cost an incredible amount of money. Who is going to pay for this? Of course the sender will pay.

Does CDN service violate net neutrality? No. why? CDNs treat packets very differently from plain Internet Service. But who is the owner of these packets? Is it you at home viewing a movie? Nope. The packets you receive are courtesy of someone that paid a CDN to host them. You request an item (a movie) by sending packets as part of your Internet Service. In this Internet Service your packets can be lost with equal probability as any other user sending email, viewing a non-CDNized movie, chatting, or whatever. But when you receive a response that is 'sponsored' by someone through a CDN, special care is taken not by your Internet Service Provider, no, do not fool yourself, it is by the resources of this 'someone' and this CDN that

special actions happen to the packets that reach you. It is not anymore 'your' service. It is this 'someone's' service what is better. But the benefit is all FOR YOU.

We can now compare CDN service to our old good Carrier Services. You can imagine that you use regular Royal Mail/US Mail/Any National mail… to request an important document from an entity (maybe even from a Government). Your request is nothing 'special' in size, urgency, quality or confidentiality so regular mail service is just OK to carry it. You are using entirely neutral service. The response to you is a very unique and valuable object/document so responder pays a Courier service to deliver urgently and securely to you. Does this violate neutrality of postal service? No, absolutely not. When you receive this high quality service you are not diminishing or subtracting resources from the regular postal service. You do not even pay anything for the extra quality, it is the sender who 'makes you a present' by enhancing the speed, security and reliability of delivery. The extra effort is done by an independent third party and this party receives extra payment which is completely fair. No one violates postal service neutrality by providing Courier Services.

Have you ever wondered if the existence of Courier companies could be violating 'postal service neutrality'? Are the DHLs and UPSs of this world 'bad people' because they make money offering better service than National Mail services? Of course they are not. At the same time you would like Courier prices to be lower if possible but that depends only on the differential quality vs National Mail and the price of National Mail.

9. Regulation

Have you ever wondered why so many people claim 'for a regulation' over many things? They want regulation over Internet behavior, over telecommunications prices, over highways, over their capacity and their pricing… We are all the time asking 'someone' to come and regulate things. No one seems to have a problem with that. Don't you think there should be limits to regulation? These claims are childish.

Regulation has had a good effect over 'public interest services', as we have said there is a fair amount of these services in our world : water distribution, postal service, energy, telephony, first aid and urgency health services (not in all countries), education (not in all countries),… .The regulator places itself above the market and disrupts the 'pure' market behavior. Of course to do this only someone with higher authority than the money can buy can take the role of regulator. Only Governments can do it and they usually do it. There are enormous differences about regulation coming from different cultures and political arrangements.

But even regulation cannot work without legal limits. In the Anglo-Saxon legal tradition the figure of 'Common Carrier' defines the limits of public interest Carrier service to be a candidate to be regulated by the Government. At least it tries to set the conditions in which a service can be considered to be 'Carrying messages for anyone without discrimination' and thus can be considered 'public interest' and be regulated to ensure that everyone can have equal access to such a service. It comes from the postal world by the way.

Another reason for an authority to intervene a service is the 'natural right' that emanates from the property of resources. For big, common, public infrastructures like the ones needed for water transportation, energy, litter, telecommunications, roads and highways, postal service… it is needed to 'take' terrain that belongs to the community and restrict it to a new usage. This capture of resources is done to serve the community but some authority that represents the community (a government) must take control of this action so at the end the community does not receive more damage than benefit.

Internet does not consume physical space (at least nothing that would bother any community). Installations of cabling may cross national borders , like trucks working for postal service do, but there is no need to make 'border checks' on information bits, as they are all born equal and harmless in the physical world. There are no national borders for telephony cabling. Companies do not pay fees to governments to cross the borders with cabling. So you start to see that there is no 'natural right' to regulate telecommunication emanating from community resources. The only reason to allow for regulation comes from 'public utility' of being connected to internet.

No one doubts today that there is a value in having access to internet. It is an economic, social, political, personal value. So internet access has become like water, energy, health, education. But at the same time notice that these important 'public interest matters' are not equally regulated all across the planet. Why would you expect that internet access will be?

10. DPI, transparent caching and communication secrecy

I have mentioned DPI as a new technology that allows breaking network neutrality (in case some router owner is very interested in breaking it).

There is bigger controversy about DPI than just allowing for unfair traffic handling. Notice that if DPI allows someone to harm your traffic by imposing a 'higher resistance' to cross the Internet, compared to the 'average resistance' that all users suffer… prior to causing this damage the one that applied DPI must have had access to information in the upper level protocols (above layer 3). This is comparable in the world of Carrier services to 'looking inside the envelope'. This violates communication secrecy. It is a major sin.

In life there are envelopes for a reason. In the outside you place information for the handler; in the inside you place information for the receiver. You do not want the handler to eavesdrop inside your envelopes. Regulation of the postal service helped not only ensuring reasonable prices and whole territory coverage so anyone has the 'right' to send and receive letters. Postal regulation also set an authority (the Government usually) protecting the secrecy of communication and is this authority who does prosecution of infringers. And this is very serious in most parts of the world.

Wired telephony inherited the protection of the postal service so telephone calls cannot be lawfully intercepted. Both services postal service and telephony have evolved to Internet. Has Internet inherited the protection of carrier services? Oh, it is difficult to tell. My first reaction will be to answer: no. Not yet. You will need to review the question country by country.

Not being a 'Common Carrier', things get messy. There are some rules out there that seem to protect 'all communications'. Out of the Anglo-Saxon world, in Europe, many countries have rules that protect secrecy in communication and that seems to cover Internet messaging. But these countries find difficulties in distributing responsibility to essentially an unknown number of message-handlers in-between sender and receiver.

One good example is 'caching services'. CDNs have been considered caching services in many regulations.

Did you know that for effective caching it is necessary to eavesdrop inside your messages? Did you know that early caching services started to do it without telling anyone and without permission of sender or receiver? For this very reason many early caching services were found as violators of secrecy and closed.

As caching turned out to be 'useful' for 'common messaging', that is, good for the sender and user in many circumstances law-makers were 'compelled' to modify the secrecy protection allowing exceptions. The 'caching exception' is translated into 'Common Carrier' laws all around as a list of circumstances that limit the purpose and ways in which information 'inside the envelope' can be accessed by the handler.

Of course this is just a 'patch' to the law. Smart people can now eavesdrop into you messages claiming they adhere to the 'caching exception' to secrecy. As any patch, this is a dirty and misaligned thing in the face of a very solid basic right that is communication secrecy.

How to overcome 'secrecy protection' to offer CDN service? Easy; ask for permission to eavesdrop to the sender. As the sender is not the one that receives traffic (a movie for example), but the one who hires a CDN to serve the movie, in the services contract there is a clause allowing technical middle-man packet inspection for caching purposes that comply with the 'caching exception' rules. The movie viewer cannot complain. The movie owner does not want to complain, he is happy about the caching.

What about transparent caching? If I do not hire a CDN… can anyone in the middle inspect my messages claiming a 'caching exception'? Of course not, but sometimes they do. Some ISPs install transparent caches. They inspect traffic from ANY source in search of clues to cache repeated content. They do not ask anyone permission to do that. Prior to 'caching exceptions' they could be considered liable of secrecy violation. Today you would need to take the laws of the country in which the DPI/cache is physically placed and carefully study the method and purpose of transparent caching. In many circumstances you will have a legal case against the one who is doing DPI/transparent caching.

Did you know that to avoid legal prosecution it is very probable that you have been made to sign a clause in your ISP contract allowing this ISP to perform DPI/transparent caching? Of course this clause does not say '…we hereby are granted permission to eavesdrop…' No, the clause will more or less say '…we are granted permission to manipulate traffic through technical means including caching under the caching exceptions to telecommunication laws…'.

The fact is that asking for permission is the best way to eavesdrop. There is a well-known company that gives you free e-mail but you allow them to classify your messages by means of inspecting everything inside them.

Another fact is that if someone does not have a contract with you he cannot ask for your permission nor receive it to look into your traffic. That is, if someone different from my ISP places a cache in the middle of my traffic (for example he caches a web page of my own, or intercepts traffic from any server at my home), or anyone does DPI on packets going out of my home, not being my ISP it is impossible that he asked me for permission, and thus I may not agree with him eavesdropping into my messages.

It is important to notice that this is happening and you can do very little to stop it. You could figure out that an ISP in the middle is doing transparent caching, find the country in which the DPI/cache is placed, find the specific law of that country, (try to) find the specific method and purpose the ISP applies and if you find yourself with enough money and strength take them to court. Honestly you do not have much hope of success.

11. Conclusion

We have seen that net neutrality is about dealing with traffic in equal conditions independently of the identity of traffic owner.

We have seen that, as of recently, technology allows to break neutrality. But the violator still needs a reason.

We have seen that Internet service is not a Carrier Service; it is not end-to-end, it is an Access Service.

We have seen that from the legal perspective, Internet Service is not a 'Common Carrier' service.

We have seen that regulators, like the FCC, cannot simply force ISPs to increase any capacity in any interconnection. We have seen it will not address congestion problems.

We have seen that neutrality is violated everyday by transparent caching and DPI. We have seen that a 'patch' has been applied to law to allow violating secrecy to a certain extent.

It seems clear that even supposing that DPI/ transparent caching is lawful (which in many cases is objectionable) , once a DPI has been performed the router owner could do other things that go beyond violating secrets. He can use the information to change the natural balance of traffic. He can prioritize at will.

This prioritization can be a net neutrality violation.

As Net Neutrality is not a law, it is not even a 'law principle', it is just a policy, that is a recommendation, no one can take to the court an ISP due to a 'creative traffic engineering', once proved that the DPI performed by this ISP was lawful (under the caching exceptions or allowed by the ISP-user contract).

It is still possible to take to the court ISPs and service providers that have not asked you for permission to unbalance your traffic and that cannot allege lawful caching exception.

Applying these conclusions to some recent cases of 'famous movie Distribution Company' vs 'famous ISP' you can see that the regulator, or the courts will have a very difficult day (or year) in dealing with their responsibility to take control of the behavior of the ISP or the behavior of the distribution company.

The most probable development of these complaints is to be judged under trade laws, not under communication laws. The courts will not feel competent to apply 'recommendations' as 'net neutrality' but they will be happy to look for contract infringements.

What is uncertain is if they will find any contract infringement. In my own view it is very likely they won't.

We can conclude that 'Net Neutrality' is an aspiration; it is not backed by law.

Net neutrality is a complex issue that requires society, companies, law and courts to mature and change.

Today Net neutrality is badly understood. I have had the sad experience to read articles, even from reputed writers and journalists that usually have a clear understanding of the topics they deal with, that completely missed the point.

They miss the point because they let themselves be abducted by rage and by a misleading comparison to 'basic human rights'. They feel it is important to do something to grant neutrality… and they fail to realize that the network is essentially neutral and someone not making his traffic through cannot claim the network is not neutral.

At the same time there are neutrality violators (DPI/transparent caching) but our society has created laws to support them. It is important to realize that these violations are serious and laws must be changed.

I hope that this long reflection about all factors involved in Net Neutrality may have been interesting to all of you.

Have a nice and neutral day.