Net Neutrality, Rest in Peace

James Mosier

Net Neutrality, Rest in Peace

GIAC (GSLC) Gold Certification

Author: James Mosier, CISSP, PMP, jim@n2truth.com
Advisor: Rodney Caudle

Accepted: September 24, 2011

Abstract

There is a war for your identifiable information. Every day, organizations of all sizes struggle with balancing the challenge of protecting personal identifiable information (PII) and the need to protect the organization from unsuspecting liabilities. It nears a religious war in passion as system administrators are put in the difficult position of balancing economic, security, privacy and legal concerns. Of the many issues, one significant issue is the opposing points of the user's rights to anonymity in use of a service they are paying for (or Net Neutrality) and the right of the provider to make content based decisions and/or prevent malicious activity via Deep Packet Inspection (DPI). This paper will cover some of the details and historical events surrounding Net Neutrality and explain why it will likely disappear sooner than most people think.

1. Introduction

No one would argue that the Internet has become an instrumental part of society. With broadband access in a large percentage of homes, WiFi freely available in many places of business, and smart phones connected via mobile service providers, our access to the information portal has become nearly an always-on experience. We have all benefited greatly from shopping, settling an argument, listening to music or watching a video and get great joy in being the first to share a particular piece of content with our friends.

This existence and exposure has transformed the Internet and all its goodness from a luxury item to a necessity for our quality of life. We have traveled down a road that has no return path without some drastic measures and impacts. Ask yourself the following questions:

How much personal information am I willing to share with strangers?

If I pay for something, should I be at liberty to use it how I please?

Am I willing to trust a company or government body with proper handling of my information?

Should we all be willing to give up more freedom in the name of security or to save some money?

These questions may sound a little extreme, but this paper will explore the forthcoming measures that could end the all you can eat buffet Internet experience and the effects that may bring about the end of Net Neutrality.

Note: throughout this paper, the word *filter* does not apply to the traditional meaning held by most system administrative and network security professionals. It instead applies to the industry agnostic meaning of merely identifying a particular entity and associating it with a predefined classification; not blocking. For this paper, it means sending data through a system that has the ability to break the

James Mosier, jim@n2truth.com

data down into classifications that represent the type of data and possibly the value of the different types to the subscriber or the provider.

2. What is Net Neutrality?

Net Neutrality is essentially the idea that as a subscriber to a network service, a user should not be subject to monitoring, restriction or filtering of the content by the provider. Most service and equipment providers have their own twist on what the principle actually means. The basis of the definition is formed from the idea that the Internet should be classified much like the stagecoach, railroad, sailing vessels or the telephone were in years past; that is to be regarded as an indispensable instrument of commerce and must be protected for the public interest (Lenard, 2006)

The promise of net neutrality is to maintain the way the Internet was originally thought of; open and a facilitator for sharing information (Licklider, 1962). As a user of many different types of Internet services, one should give no thought to the filter of one content type over another or whether the data associated with usage is being captured and stored. Most would agree that if their usage was measured for the types of content and being billed differently on that type, or if their data was simply being stored, they would consider and likely adjust their usage; much like rising gas prices or new tolls change our driving patterns. The possibility of a non-neutral Internet negatively impacting innovation and creativity in network services is a risk our society should consider very carefully. (Mehlan, 2009)

Proponents of net neutrality argue that the network itself is simply infrastructure that should not add value to the service, and thus innovation should occur only at the edges of the network (Lehr, 2009). For most is will likely come down to whether or not I should expect privacy when subscribing to an Internet service.

2.1. Open Internet

The concept of Open Internet is starting to morph as well. Back in 2005 the Federal Communication Commission (FCC) defined Open Internet as any lawful content, any lawful application, any lawful device, and any provider. (FCC, 2005) It is worth pointing out that this policy statement does

not take a firm position of nondiscriminatory, but uses the word lawful over and over; which is open to interpretation.

A typical Internet connection under this definition would look like figure 1 and have no regard to the content or destination regardless of the provider as long as the content is considered legal.

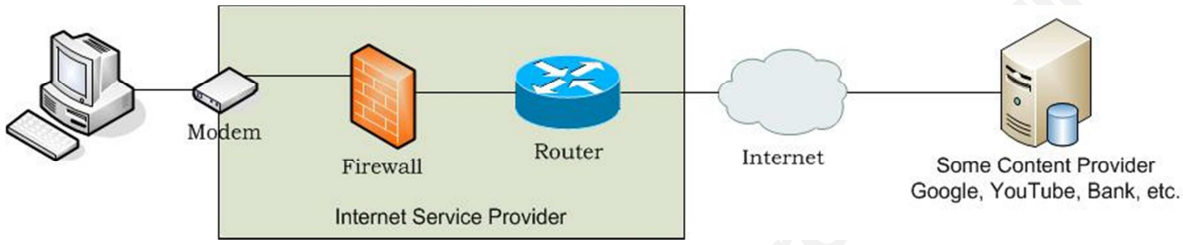

Figure 1

2.2. FCC

The previously mentioned, 'no unlawful restriction' position has been gathering more and more followers over time since it was a campaign promise of then presidential candidate Barack Obama. (Bosker, 2010) To his credit, President Obama supported this promise with his appointment of FCC chairman Julius Genachowski; a well know advocate of net neutrality. A new set of proposed rules governing the Internet was introduced by Mr. Genachowski soon after his appointment. (Singel, 2011)

Recently, the FCC published their official position on what an open Internet looks like. This plan will face challenges by both the business sector and watchdog organizations over the FCC having jurisdiction and authority to enforce Internet policy. Verizon and other providers have already stated they intend to file a notice of appeal. (Melvin, 2011) Additional lawsuits and congressional challenges on the FCC order are expected.

2.3. Comcast

The first national attention getting event on net neutrality was not so much a neutrality matter, but rather a throttling issue. In 2007 Comcast was accused of throttling peer-to-peer traffic. They promptly denied the charge, but have been in a battle with the FCC ever since. (Gross, 2011) Comcast went further to challenge the FCC authority to enforce the policy even though if denied blocking anything. (Jones,2011)

2.4. Verizon / Google

In contrast to the alleged Comcast method of applying a gate keeper stance, Verizon and Google are trying a different approach. In a recent joint statement from Verizon and Google on the Verizon policy site, Tom Tauke, Verizon Executive Vice President of Public Affairs, Policy and Communications he states (Tauke, 2011),

> It is imperative that we find ways to protect the future openness of the Internet and encourage the rapid deployment of broadband. (Tauke, 2011)

This statement was primarily in response to Mr. Genachowski's governing rules proposal. Reviewing the entire Verizon / Google proposal leaves a great deal open to interpretation. It seems to be establishing the groundwork for a tiered Internet when considering the rest of Mr. Tauke's post.

> Broadband providers would be required to give consumers clear, understandable information about the services they offer and their capabilities. Broadband providers would also provide to application and content providers information about network management practices and any other information they need to ensure that they can reach consumers. (Tauke, 2011)

> Our proposal would allow broadband providers to offer additional, differentiated online services, in addition to the Internet access and video services (such as Verizon's FIOS TV) offered today. (Tauke, 2011)

James Mosier, jim@n2truth.com

Verizon's statement indicates interest in playing both sides of the debate. One thing is clear in their argument; their goal is a two-tiered Internet with one tier being open as they define it and the other being more business centric.

It would be easy to think of Verizon as the evil twin in the partnership, but Google has some dirty laundry to be considered as well. The number of ways that Google collects PII is incredible. Your web searches (Google), your reading habit (Google Books), your email (GMail), your phone calls (Android) and voice prints (Google Voice), your family pictures (Picasa) and the list goes on. With Google's zealous efforts to fulfill its stated mission of "organize the world's information" and "make the collection of personal information transparent**"** (Google Philosophy, 2011) it takes a great deal of effort for a person to remove their personal information from Google's Repository. Google was singularly identified as public enemy number one and a hostile actor against privacy by Scott Cleland in his book, Search & Destroy: Why You Can't Trust Google Inc. (2011)

2.5. Illegal Activities

Opponents to the neutrality position have plenty of ammunition. One opposing position to net neutrality is the opportunity it continues to present for illegal activities. Over the years many applications, protocols and even websites have been developed with little ground to stand on other than to commit illegal activities as defined by US laws. (SIIA, 2011)

Some of the more popular:

- Network News Transfer Protocol (originally a noble effort)
- Napster
- Gnutella
- BitTorrent
- Pirate Bay

James Mosier, jim@n2truth.com

Recent lawsuits and threats of liability have led many universities and corporations to expand their network terms of use to prohibit certain websites and protocols that may be used to violate copyrights. (Cheng, 2007)

3. Deep Packet Inspection

Deep Packet Inspection, or DPI, is defined as the inspecting of the payload of data to determine its content and potentially making a decision based on the result (Porter, 2005). A typical placement of a device capable of processing packets in either real time or collection for processing later is shown in figure 2. In most cases the DPI device would be on a switch SPAN port and may sit in one of many places in between proxies, routers, switches and firewalls depending on the provider's network configuration.

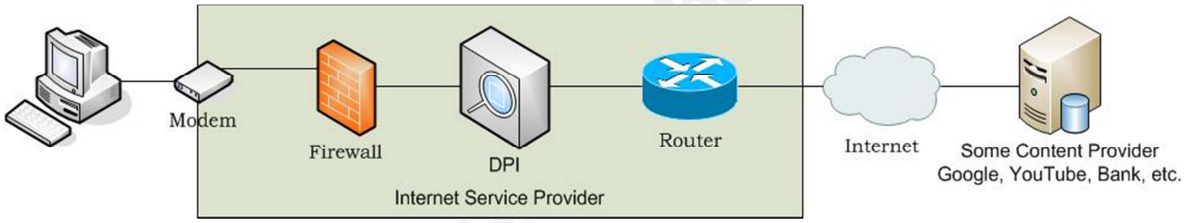

Figure 2

The purpose of the DPI device is to analyze the content of information transported by the network and then make a decision based on the result. This may sound like Quality of Service (QoS) at some level, but most QoS decisions are made by the determination of the protocol used, not by the data within the packet. Where QoS typically operates at layers 2 and/or 3 of the OSI model, DPI can operate from layer 2 all the way through to layer 7. See figure 3.

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Figure 3 – OSI Layers

James Mosier, jim@n2truth.com

Consider the conceptual packet diagram in Figure 4. QoS would typically see the protocol section of the packet and might identify the pack as a voice over IP packet. It would then instruct the routers to treat the packet with a higher priority to ensure good voice quality. DPI opens the door to inspecting the data or content portion of the packet and handling or billing the packet differently based on rules defined by the service provider. DPI might identify the data as a video or music over http and meter the transmission for a higher charge than email.

Figure 4 – VoIP Packet

The only type of DPI usage that most are willing to submit to is legitimate, warranted surveillance by law enforcement in the process of a crime. (NoDPI, n.d.)

3.1. Corporate Investments

When thinking of DPI, the position of the larger providers should not be over-looked. Verizon, AT&T, Comcast, Time Warner and others are constantly investing significant dollars (Verizon Wireless, 2009) to expand the bandwidth and reduce the Internet latency of their network subscribers. As with any sustainable business model, new services and revenue are required to maintain and grow. For society to expect the providers to continue to expand the capacity without new streams of income is inconceivable (Reiner, 1987).

3.2. Types of DPI

There are essentially two basic methods of DPI (Solera Networks, 2007). The first, and more costly, is real time DPI. This form involves inspecting the packets as they traverse the network and requires significant processing and complex network design in order to prevent too much network delay. The alternative to real-time would be storage; also called Deep Packet Capture. Storage would

impose a greater risk to privacy as the data is maintained somewhere for later analysis. Regardless of the method, the goals of DPI are broad; here are several of the most common.

3.2.1. Behavioral Advertising

Other than the obvious custom ads we all have seen from Google, Microsoft and Yahoo, there is an opportunity for much more to happen behind the scenes. One example is NebuAd. Though now defunct, NebuAd was a small company that operated on a business model that could not have existed a few years ago. The offering from Nebu was to assist ISPs in determining end user behaviors to target the marketing of specific ads to the user. NebuAd faced many challenges from various watchdog entities and privacy advocate groups asserting their technology was in violation to the federal Wiretap Act. (U.S. Code, 1986)

One of the most vocal challengers to companies like NebuAd is Alissa Cooper, Chief of Computer Scientist at the Center for Democracy and Technology. According to Ms. Cooper, "In many cases, DPI equipment will automatically collect personal identifiable information." (US House 110–137, 2008)

3.2.2. Determining Intent

Proponents on the DPI side of the argument have a great deal of ammunition to back up their position. They could argue the user needs protection to prevent privacy violations, identity theft, child pornography or other forms of illegal or immoral activity. The issue of what is illegal and where it is illegal and who has the authority to impose a policy still needs to be answered. Even if we knew the answer to those questions there is the more serious matter of how your usage may be interpreted. (US House 110–137, 2008)

With DPI being based on classifications, rules, signatures and other variables, it is only as good as its defined set of instructions. Dr. David Reed of the Massachusetts Institute of Technology

proposed in his testimony to Congress in 2008 that Deep Packet Inspection is attempting to determine your intent by either collecting your information or guessing. (US House 110–137, 2008) Have you ever ended up on a web site you did not intend to and would otherwise find offensive or inappropriate? What if that data stream was collected to determine your intentions?

Without the preservation of Net Neutrality, we may have a future were we will need to put more thought into out bookmarks, clicks, subscriptions and such. The energy and effort spent by a person to avoid such tracking will certainly have some impact on productivity. Recently in Egypt, many users have resorted to using the Tor network in an effort to appear anonymous with their information. (ioerror, 2011) A popular method to employ Tor usage is through a device like an Ironkey. (Ironkey, n.d.) Fear of being monitored and the repercussion associated with some data has created an incredibly messy Internet infrastructure in Egypt. (ioerror, 2011)

3.2.3. Congestion Management

Providers have a valid case that data stream inspections are needed in order to manage congestion and make routing adjustments based on real time demands. This is the type of DPI that most subscribers would take no issue with as they are likely to benefit from its results. (Lehr, 2009) During a high traffic condition, a provider could then choose to route higher consumption traffic to an alternate path to permit normal traffic to avoid impact. With this type of DPI we should expect to pay a premium for those higher consumption uses; much like power companies do today with load balancing.

3.2.4. Service Tiering

There are many issues to consider when thinking of employing a model where packets are inspected and categorized. One of the biggest concerns is the prioritization based on some model that we may not agree with. For example, recently in Japan after the great earthquake struck, many folks had an extremely difficult time getting to the airport. Once they arrived, they were further challenged

at how long the lines were to speak to someone about getting on a flight. Now imagine there was a much shorter line than the others, but in order to use that line, you must be part of priority club.

Appling that perspective to the Internet where one may be required to embrace a more closed environment with restriction and rules to comply with in order to get better performance. (Lehr, 2009)

Suppose you use your phone to read your email, check your calendar, stream some music, read a blog and get some directions to the theater. If your carrier were to suddenly implement a metering policy charging a premium for one or more of those types of requests you might feel like you have been baited or even trained into becoming a certain type of user that can then be charged more.

If the service providers hold to their pattern, then we should expect to see a lengthy user agreement with terms of use and a long legal explanation how the consumers will be affected. So even though choices may be available, we will likely see a future where there is no choice for bandwidth that is not tiered, much like we are now seeing the unlimited plans begin removed as an option. (Telesmartphone, 2011)

4. Major Issues

The Internet will likely have to submit to some form of DPI, but there are some major issues that need to be addressed. As mentioned before, the methods applied to networks already by technologies like QoS or Firewalls differ from DPI. DPI does not make a decision based on a port or protocol, but rather the data content. This difference raises some rather significant issues.

4.1. Vague Privacy Legislation

Recent cases and debates on the subject of DPI are still largely based on The Cable Communications Policy Act of 1984 and The Wire Tap Act of 1968. These articles were obviously fine for their time, but with the advent of what some providers may title unintentional storing of PII, our legislation may need some strengthening to ensure our interests are protected. We will certainly see some less

scrupulous companies take advantage of short comings or loop holes in the laws. Already we have seen Comcast (Gibbs, 2009) and Google (Bukher, 2011) pushing the envelope.

.

4.2. Entrepreneurship

The issues in the area of entrepreneurship are a double edged sword so to speak. We could certainly see an increase in technology from equipment manufacturers if the concept of DPI experiences some momentum; just like we have seen in in the past. In direct contrast, there is a risk that DPI will impact innovation and creativity if usage of network services are restricted due to fear of information loss, increase in cost or are subjective to automated anti-competitive bias in the operation of the network. Unfortunately, we are already seeing a negative impact of such policies in some countries like China and Saudi Arabia. . (NoDPI, n.d.).

4.3. Opt out Policy

The trend we are seeing as Internet consumers, is the providers and businesses that want to collect information for a given purpose are attempting to gain our consent through an – opt-out position. This means in order to be excluded from a packet inspection operation, I must take action even if I am not notified of the inclusion. (Balasubramani, 2011)

4.4. White/Black Listing

White listing and black listing are terms used in many network based services. A white listed item is identified as acceptable. Conversely, a black listed item is identified as unacceptable. (TechTerms, n.d.)

If such a methodology is applied to network traffic in the form of DPI, the risk of some service no longer being available will become a reality. A service could be identified as unacceptable even though there may be valid uses for it. This environment would require an exception process and would force the end user to request an exception. We then have to ask the question, who decides? What would be the process for white listing newer technology?

James Mosier, jim@n2truth.com

4.5. Enforcement Body

Another problem yet to be solved is how data that crosses governmental boarders should be handled. Imagine you stream music from your favorite site that happens to be in a different country. If you and the others subscribers were to suddenly stop using the service, due increased cost imposed by your service provider or your government, the content provider would lose their customer base and have a grievance with the body that is enforcing the filtering policy.

World governments will have a very difficult and long process of determining how an oversight body could be established and maintained. Once that hurdle is cleared, then the matter of authority of such a body comes into question.

Service providers typically use an acceptable use policy, but this agreement is between the end user and the provider and not from the end user to the destination. The destination of any connection will have a provider that may have a totally different set of policies and definition of what is acceptable and chargeable at a different rate.

This issue is one that cannot be resolved by one government. If DPI is universally deployed, an international body will need to be established that is afforded jurisdiction by the participating countries. This body will then have the difficult, if not impossible, task of establishing and enforcing DPI policies across borders.

4.6. End User Burden

A typical end user will find the technical options available to maintain privacy and anonymity fall short when considering ease of implementation and scalability. Even a savvy user will become frustrated at the effort required to achieve small amounts of privacy in a DPI environment. Key exchanges, secure protocols, client/receiver configurations and coordination with recipients are just a few of the complex steps required to establish a secure, private, point to point session; never mind a meshed environment.

James Mosier, jim@n2truth.com

Internet users searching for a solution to defeat DPI may resort to a something like a VPN subscription service. (Young, 2009) This may work well for shielding a user from a snooping ISP, but it will fall short if the VPN provider has their data compromised, stolen or requested by a court. Additionally, we have no guarantee the VPN provider is not storing data that could expose PII. In fact, even if the VPN service is solid, many Internet sites are capturing origination points upon each visit, and then attempting to establish a session with the originating client. (See Figure 5) Some sites will have many sub-sites or partners they allow to capture the same information as well. A user wishing to put forth an additional defense to shield against this potential exposure will need to employ some local filtering software like PeerBlock. (PeerBlock, n.d.) These two additional complex steps, still do not guarantee anonymity.

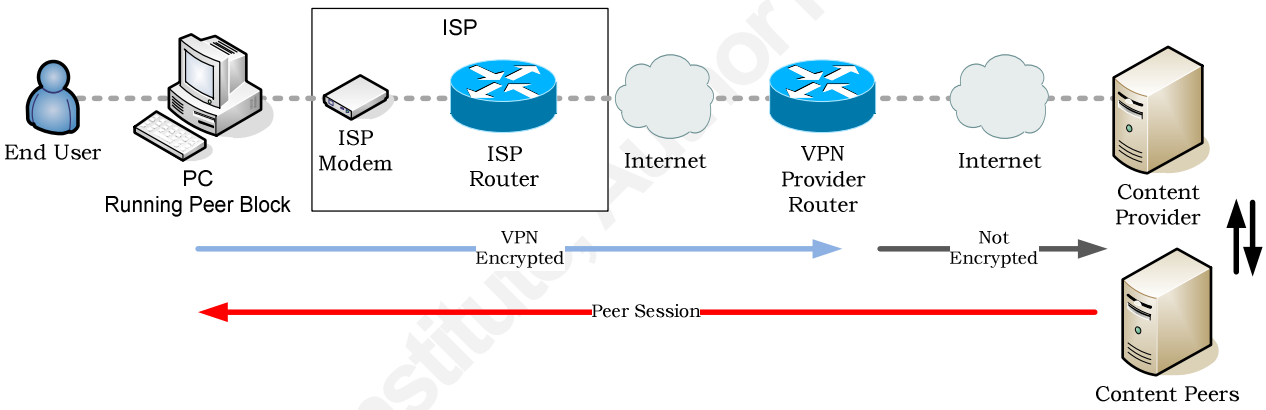

Figure 5 – End User Challenge Illustration

5. Conclusion

The war of privacy verses security has been at odds since the beginning of the Internet. The battle between Net Neutrality and Deep Packet Inspection is shaping up to be significant and may remove the consumer's ability to remain anonymous while using a service they pay for. Further complicating the issue is the lack of standards, policies, governance and acceptance of DPI.

James Mosier, jim@n2truth.com

Whether a person is more concerned over the privacy risks, the potential impacts to innovation, the opt out policy, application black listing or being subject to a governing body that will impose unilateral policies, the reality is that some form of DPI is in our future.

Though Deep Packet Inspection is able to perform a great deal of analysis across the different layers of the OSI model, the only form currently recognized as acceptable is in the warranted act of surveillance by a law enforcement organization. This small level of acceptance is not enough to discourage service providers from experimenting and planning a future broad use. Service providers need to implement a certain level of analysis to maintain the network systems of the Internet, but they do not need to analyze the data payload and potentially store it for future analysis.

In a DPI world, the end user is faced with no sustainable technical solution to address the concerns over an entity having the ability to inspect or collect data. In the absence of a technical avenue, user community awareness and government oversight is required to provide some level of protection.

6. About the Author

James Mosier has been involved in various levels of Information Technology since 1984 with Jones Intercable, U.S. Air Force, MCI and Verizon. He is currently the senior program manager handling complex communication integrations for international companies supported by Verizon.

7. References

According to ibiblio. (n.d.). Internet Pioneers. Retrieved from http://www.ibiblio.org/pioneers/licklider.html

Balasubramani, Venkat. (2011). Deep Packet Inspection Lawsuits: NebuAd Partner ISP Wins Summary Judgment -- Kirch v. Embarq. Retrieved from http://blog.ericgoldman.org/archives/2011/08/deep_packet_ins_1.htm

James Mosier, jim@n2truth.com

Bosker, Bianca. (2010). Watch Obama's Net Neutrality Promises, Promises. Promises. Retrieved from http://www.huffingtonpost.com/2010/08/13/net-neutrality-obama-see_n_681695.html

Bukher, Tim. (2011). Google's Wiretap Argument My Bring About de facto Net Neutrality. Retrieved from http://www.handalglobal.com/2011/04/googles-wiretap-argument-may-bring-about-de-facto-net-neutrality/

Cleland, Scott. (2011). Search & Destroy: Why You Can't Trust Google Inc. St. Louis, Missouri: Telescope Books

Federal Communication Commission. (2005). Policy Statement. Retrieved from http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf

Gibbs, Colin. (2009). FCC Fires Back at Comcast in Net Neutrality. Retrieved from http://gigaom.com/2009/09/21/fcc-fires-back-at-comcast-in-net-neutrality-legal-battle/

Google. (2011). Google Corporate Information: Our Philosophy. Retrieved from http://www.google.com/about/corporate/company/

Gross, Grant. (2011). Court: FCC Had No Authority to Stop Comcast's BitTorrent Restrictions. Retrieved from http://www.pcworld.com/article/193574/court_fcc_had_no_authority_to_stop_comcasts_bittorrent_restrictions.html

ioerror. (2011), Recent events in Egypt. Retrieved from https://blog.torproject.org/blog/recent-events-egypt

Ironkey. (n.d.). Private Surfing. Retrieved from https://www.ironkey.com/private-surfing

James Mosier, jim@n2truth.com

Jones, K.C. (2011). Comcast Chided For Managing BitTorrent Network Traffic. Retrieved from http://www.informationweek.com/news/202600785

Lehr, Willaim H, & Pupilo, Lorenzo Maria. (2009). Internet Policy and Economics: Challenges and Perspectives. New York: Springer Science + Business Media, LLC

Lenard, Thomas M, & Randolph, J. May. (2006). Net Neutrality or Net Neutering: Should Broadband Internet Services Be Regulated. New York: Springer Science + Business Media, LLC

Melvin, Jasmin. (2011). U.S. "Net neutrality" rules to take effect in November. Retrieved from http://www.reuters.com/article/2011/09/23/us-fcc-netneutrality-idUSTRE78M4AS20110923

NODPI. (n.d.). FAQ. Retrieved from https://nodpi.org/faq/

Peer Block. (n.d.). FAQ. Retrieved from http://www.peerblock.com/docs/faq#is_it_working

Reiner, Rob. (Producer & Director). (September 1987). *The Princess Bride* [Motion Picture]. United States: ACT III Communications

SIIA. (n.d.) Internet Piracy. Retrieved from http://www.spa.org/index.php?option=com_content&view=article&id=337&Itemid=350

Singel, Ryan. (2009). FCC Backs Net Neutrality — And Then Some. Retrieved from http://www.wired.com/epicenter/2009/09/net-neutrality-announcement/

Tauke, Tom. (2011). Joint Policy Proposal for an Open Internet. Retrieved from http://policyblog.verizon.com/BlogPost/742/JointPolicyProposalforanOpenInternet.aspx

TechTerms.com. (n.d.) Blacklist. Retrieved from http://www.techterms.com/definition/blacklist

James Mosier, jim@n2truth.com

TechTerms.com. (n.d.) Whitelist. Retrieved from http://www.techterms.com/definition/whitelist

Telesmartphone. (2011), Verizon to Stop Offering Unlimited iPhone Data Plans this Summer? Retrieved from http://www.telesmartphone.com/2011/03/04/verizon-to-stop-offering-unlimited-iphone-data-plans-this-summer.

The Cable Communication Act of 1984. (1984). Titile VI - General Provisions [Data file]. Retrieved from http://www.publicaccess.org/cableact.html

U.S. Code. (1986) Title 18 (Wire Tap Act). Retrieved from http://www.law.cornell.edu/uscode/usc_sec_18_00002511----000-.html

US House 110–137. (2008). What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies [Data file]. Retrieved from http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg58071/pdf/CHRG-110hhrg58071.pdf

Verizon Wireless. (2009) Verizon Wireless Surpasses $1 Billion Network Investment in Indiana. Retrieved from http://www.redorbit.com/news/technology/1741726/verizon_wireless_surpasses_1_billion_network_investment_in_indiana

Young, Julian. (2009). Bypass Deep Packet Inspection. Retrieved from http://www.julian-young.com/2009/11/30/bypass-deep-packet-inspection/

James Mosier, jim@n2truth.com