

The Internet Ontology: Why Punish Success?

Esmond Kane: Student
lstue120 : Class
5/23/2006 : Date

A user clicks a link in a web browser. In a mechanical analogy, a lever, a trigger is pulled and the request passed up a chain of trust. Software intervenes and the click is interrogated to determine the nature of the request¹. More software is called and the data “packet”² is placed onto a network and converted into electric pulses.³ The user is no longer involved once the packet is placed on the network. The packet and the users delivery request is subject to the contractual agreement negotiated with the network provider. The user has no further recourse to action or control over the information submitted.

Not all software is the same. The underlying principle behind the current generation Internet is that of *Network Neutrality* and *Edge Intelligence*. Put plainly, vendors agree to interrogate network traffic only at intelligent “End Points”⁴ and network traffic is inviolate, accepted at face value, with an agreed “public” envelope and most importantly, free from bias. This established hierarchy of trust and the politics of inter-exchange facilitates communication across alien software and hardware and across vendors and nations. Core to this established chain of trust is the reliance on standards. We rely upon standards to baseline the communication framework in a neutral fashion.

So where has the users packet really gone? The contract negotiated with the Internet Service Provider means the provider will attempt to “route” the packet to its destination. Custom network hardware intervenes, peels the source and destination address from the packet and rewrites it to optimize the transfer. The packet header is like an envelope,⁵ and like the Postal Service, the I.S.P. agrees to only work with “public” information contained in the packet header, written on the envelope. All along the transmission chain, the packet header is rewritten, the older packet encapsulated in the new, like an “onion” only the topmost layers are accessible without compromising the integrity of the whole. The path taken may involve alien hardware, software from multiple vendors, different revisions of software,

1 Web browsing inherently involves requesting information stored on a remote machine

2 A Packet is data, an application request or content, prepared into a network-ready digestable stream

3 Application requests are encoded into application code and addressed for the destination service at the users behest

4 Typically computers or workstations

5 To facilitate understanding, I will use header and envelope interchangeably to refer to a protocol or packet signature

the only commonality is the agreed standard for facilitating exchange, the Internet Protocol. ⁶

Eventually the packet arrives at the destination and is passed up another software chain to the Server Application where it is interpreted and a response crafted based on the request and addressed to the original “source” revealed beneath several layers. This transmission and communication process occurs again and again, thousands of times a second.

The core concept behind the neutral network, this standardization of information exchange, is under threat. The big Telecommunication Providers⁷ want more say in the formatting of the underlying content. They have asked the U.S. Government to grant them the right to treat packets preferentially based on the content. This paper seeks to confront the rationale behind the “Tiered Internet” proposal and to argue that compromising the integrity of network neutrality poses grave concerns for privacy.

The Internet Software

The military pioneered the exchange of information between computers. The whole idea of a network was developed in partnership with BBN⁸ on a contract with the Department of Defense. The initial military network⁹ was mirrored by ones built in Academic Institutions, the research areas where network development was pursued. The systems were initially homogeneous, the same software, the same hardware and only a building or campus reach. Eventually researchers extended the network concept to include networks of networks and sought to confront the problem of exchanging information between networks based on different fundamental designs or architecture. Ad-hoc standards bodies were formed to discuss the development of Internetwork exchange and a common protocol specification for the exchange. The military soon tired of the process and built a private network.¹⁰

⁶ RFC 791

⁷ Abbreviated to Telcos or Service Providers throughout

⁸ Bolt, Berenek and Newman developed the concepts behind packet switching for networks

⁹ The first network, the ARPANET was built for DARPA by BBN

¹⁰ MilNet

They donated the remaining intellectual property investment to the public, given it would be subject to the U.S. government who had funded the effort

Initially the physical lines which connected the network of networks were expensive (and slow), laid coast to coast by hand and only connected large institutions who could justify the expense, the Ivy Leagues¹¹ and the Engineers academies.¹² The existing Telephone companies already laid coast-to-coast line for telephones and lobbied for subcontracts to lay the physical pipes. Inevitably the Telcos¹³ soon owned the lines and leased connections to Institutions which paid for access. Monetary economies were negotiated and fees levied for flat-rate and variable access to these connections.

It wasn't enough, the Telcos also sought to intercede in the data transmission framework. The Higher-Ed bodies proposed an Internet Protocol¹⁴ based on a "Commons"¹⁵ model for dynamic or "Free Market" use of the available "bandwidth." The Telcos looked to their existing rigid stratified telephone standards and proposed a carefully designed "OSI"¹⁶ model for exchanging and metering growth within an accounting framework. Both bodies were attempting to account for access and growth across platforms, in one we have a body proposing their standard based on a century of homogeneous development using 1 hardware (the telephone), 1 (telephone) network and a traditional billing cycle, in the other we have a complete rejection of any hardware tie-in, network tie-in, a "laissez-faire" service guarantee and overall, a reliance on standards to account for growth. Surprisingly,¹⁷ the Telco's lost and the neutral network concept was adopted.

11 Harvards Internet was routed to the NorthEast Academic Regional Network, NEARNet.

12 The National Science Foundation Network NSFNet integrated the Academic nets

13 Telephone companies embraced the new technologies and were re branded as Telecommunication Companies or Telcos.

14 Abbreviated to I.P. throughout

15 A Commons is an archaic form of referring to a shared resource available to any and all members of a Community

16 The Open System interconnect model was an abstract design for a communication framework which heavily favoured the Telcos existing business models.

17 Given the upstart pretender defeated the entrenched incumbent

The Internet Hardware

Trying another tactic, the Telcos chose another battleground: communications hardware. It was a clear field, the Internet Standards bodies had by now incorporated into the Internet Engineering Task Force¹⁸ but still concentrated on software standards. The packets were still being routed through the Telcos network and they still favoured in-house developed standards based on “cells” and guarantees of service levels. The Telco routing was a hybrid of software and hardware standards, typically, the I.S.Ps encapsulated the defacto I.P. standard in their preferred software protocol and on top of their custom hardware. At the end of the 80's, the Telco's defacto standard was the Asynchronous Transfer Mode¹⁹ framework. ATM allowed the Telcos to meter companies access and facilitate the growth of their network at acceptable levels. To concede ground for smaller ISPs, the Telco's built dedicated Peering Points or Points of Presence as “Carrier Hotels.” These rudimentary exchange points became known as the “backbone” of the Internet.

Meanwhile, Local Area Network technology development was proceeding at a breakneck pace. Freed from the integration conceits of the Telcos, the early LAN pioneers were Ethernet²⁰ and Token Ring²¹. Ethernet quickly outpaced Token Ring. IBM “owned Token Ring and were often accused of interference and a reluctance to delegate responsibility in the design. The early Ethernet adopters, Cisco, Bay Networks, Cabletron, 3Com were able to pour capital into cheaper fabrication of specification-compliant hardware and less on fighting for standardization. In the time it took Token Ring to grow from 1-16Mbps, Ethernet grew from 1-100Mbps. Worse again, in the time it took ATM to grow from 1-45Mbps, Ethernet grew from 1-10000Mbps.

18 Formed in 1986

19 Abbreviated to ATM

20 IETF standard 802.2 and 802.3

21 IETF standard 802.5

The Backbone

Smaller I.S.P.s took note, Local Area Networks based on Ethernet could be deployed faster than Token Ring. Why not long distance? Metropolitan Area Networks based on Ethernet were proposed. Peer points served to exchange and encapsulate Ethernet, the physical layer was made irrelevant when encapsulation took away the physical limitations of the underlying medium. Rapidly, 3rd party Internet Providers arose to challenge the traditional Telecommunication Monopolies and by the end of the 90's, it was estimated the 90% of the internet was unused “dark” fiber, laid by these mayfly providers, prepared for the perceived demand of the new economy, Economics 2.0. Unfortunately the demand wasn't there, the public's adoption of the Internet was behind that of Corporations, the “wiring of America” was a railroad boom and a dramatic failure. The Telcos were able to wait it out and buy all of the property of the new economy at bargain fire-sale prices. Overnight, the Telcos owned the backbone even when they had only marginal influence in its creation and building.

ATM was a spectacular failure when Ethernet was cheaper to deploy and you could build intelligence into the Edge to convert and encapsulate. I.S.P.s ran optical fiber, copper, coax into their exchange points. There was little effort to design a physical infrastructure, the routing capabilities of the software and neutrality agreements promoted carrier neutrality. Of course, the providers were still competing for the “last mile”, the connection to customers. Frequently, Service Providers ²² use their penetration in Peering Points to add credence to a claim of being the Internet Backbone. It's a fallacy, the routing infrastructure is dynamic and does not predispose any one network or any one carrier, there is no nebulous backbone. The only truth in their claims is that the collapse in 3rd party providers and rapid mergers and acquisitions have re-incarnated the Telcos into something akin to the Bell²³ monopoly predominance.

²² MCN ran a marketing campaign specifically claiming to be the Internet's Backbone

²³The AT&T (or Bell) telephone monopoly was broken up by the Department of Justice in 1984. Some believe it now exists as a loose framework of 5 Baby Bells which dominate the U.S. telecommunications industry

The Law

The Internet became very contentious early in its founding. The approach of a Darwinian proving ground for software, the “rough consensus and running code” model was extended to the business model. Unfortunately, this “frontier” mindset butted into legal problems. Law enforcement needs ways to establish revoke-ability and authenticity. The cliché of the Internet was that “On the Internet, no one knows you're a Dog.” Cyber-Crime could be anonymous and who was responsible for revealing the paper trail anyway? It was quickly determined that I.S.Ps only facilitated the content that the new businesses and users participated in. They were prevented from intruding into the datastream by privacy protections and the standards bodies. They were unable and unwilling to police the content anyway. The idea of a “safe harbour” protected Service Providers from the abuses of their clientèle.

Existing Internet legislation relies heavily upon the Safe Harbour concept. The CDA²⁴ specifically stated in Section 230 that “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” The DMCA²⁵ further grants providers the protection of a “takedown”²⁶ notice to facilitate removing contentious material from a hosted site. Obviously providers should not be liable for the infringement of their users but its also clear that the providers must facilitate measures to enable Law Enforcement on the Internet and explicitly the CALEA²⁷ legislation specifically requires Service Providers to facilitate legal wiretapping. Counter to this pro-Telco trend in 2000²⁸ and 2005²⁹, the definition of an Safe Harbour was amended to exclude businesses and Online Providers who promote and facilitate infringement. The 2001 Patriot Act also extended the burden of service providers to respond to Law Enforcement intusions.

24 Communications and Decency Act was Title V of the 1996 Telecommunications Act

25 The Digital Millenium Copyright Act was made law in October 28, 1998

26 A Takedown notice is an document alerting a provider that it is hosting a users content which *may* infringe CopyRight

27 Communications Assistance to Law Enforment Act of 1994

28 The Napster Peer to Peer music site was shutdown after a March 2001 ruling that it facilitated CopyRight infringement

29 The Grokster Peer to Peer site was shutdown in November 2005 after a rulling that it aided CopyRight infringement

Internet legislation and its interpretation is based on the standardization framework adopted during the design of the Internet. Networks are *neutral* and usually provided by an unknowing third party or multiple parties. Providers have no say in the traffic passing across their network and are bound by privacy law not to interfere. The Internet is a commons, a library and the Government sees it as a natural resource, steered by Business. The Intelligence of the Internet's is implemented at the *Edge*, it is the users. Users are directly responsible for their content and behaviour, not their unknowing provider.

The Future

The Internet is converging. The growth of the Internet has proved that Bits are Bits, it's all one big encapsulated network. The most recent development is Voice over Internet Protocol ³⁰ in which Audio communications are compressed, encoded and transmitted over the same network formerly reserved for static content.³¹ It relies on the concept of an ad-hoc Best-Fit Committed Information Rate.³² VoIP proves the current generation Internet can contain a robust infrastructure, a reliable model and it doesn't require any further expensive outlay. The Internet is reliable enough to deliver a sustained throughput sufficient for a telephone conversation without having to lay an end-to-end physical pipe (or negotiate an equivalent guarantee). The robust infrastructure is capable of dispensing with the kind of service guarantees which the "old" telecommunications companies used to build the telephone network.

The Convergence concept is working. Service Providers are flooding clients with tempting service offerings and ever-increasing bandwidth to meet the requirements: Vonage,³³ bundled wireless, VoD,³⁴ FTTH,³⁵ MegaModemMachX ³⁶ etc. Massive effort is underway to uplift the capacities and capabilities

30 Abbreviated to VoIP throughout

31 VoIP is based in the Session Initiation protocol, another IETF framework

32 A CIR is a minimum bandwidth guarantee negotiated with an ISP

33 Vonage is a Verizon VoIP offering

34 Video on Demand plays in the same arena as VoIP and logically integrates TV, Phone and Internet onto one network

35 Fiber Optic to the home cabling can offer the potential "last mile" forward extensibility the Internet has been able to leverage with encapsulation

36 RCN label their Internet Cable Service MegaModemMachSPEED and run marketing campaigns based on how they increase service speed without requiring a financial outlay

at the core and last mile. Peering hotels and Internet Exchange Points are spawning rapidly at perceived critical junctures to reinforce the (nebulous) backbone. In reality its just more Telco “land-grabs” to secure market share and penetration. One big scramble to “own” the consumer and dominate the market.

The Telcos planned to skip the “fat-client”³⁷ paradigm with the Cellphone. Cell-phone networks allow traditional providers to retro-fit their voice monopoly to the Internet. End-points are now phones and users are locked into their providers “walled-garden.”³⁸ Content is served and approved by the provider. Access is carefully metered and billed accordingly. While the Internet existed as a data medium, the Telcos scaled the telephone network to greater heights and greater profits. The consumer still viewed the telephone and TV as separate services. When possible the Telcos used regional legislation to deter competitors. Many states have Emergency Service legislation to guarantee calls to 911. This has been surprisingly effective in preventing convergence and even prevented VoIP providers from operating and routing data in certain regional networks. However, VoIP directly encroaches upon the natural monopoly of the “old” telecommunications companies. The rapid unplanned convergence of voice, video and data onto one pipe has completely flanked their plans for dominance.

To a great extent, the Internet grew in the governance vacuum that the Telcos scorned in favour of the Telephone and now Cellphone market. While AT&T and the ITU³⁹ licensed and steered ATM and the OSI model, the IETF gave away IP and Ethernet and rang the bell for the boxing match. Ethernet quickly scaled to 10Gigabit while ATM was languishing at 45Mbit, IP became the dominant Internet Protocol, extended and twisted beyond recognition while OSI served only as a Intellectual model and conference topic. They bought the Internet pipes and inherited a thriving community built despite their non-participation. They didn’t build the Internet, dabbled in the standardization process and started up a

37 Fat Clients is a derogatory term for end points or workstations which are bloated with capabilities

38 A Walled Garden is a term used to describe an information system closed to outsiders

39 The International Telecommunications Union is an international body of Telcos

competing paradigm when their standards were rejected.

The Future in Peril

The Internet is an eco-system, an Ontology.⁴⁰ The Telcos have secured a stranglehold over the US Internetwork and they are complaining of the burden of regulation and lobbying Congress for greater control of “their” network.⁴¹ The Telcos have always argued that the Government is not facilitating access to a “public commons” but rather intruding on their business model. In question is the Telcos wish to “double-dip”⁴² and implement a business model based on extorting content providers to ensure that content is viewed seamless by users. The proposal is called the “Tiered Internet” and the Telcos speak of “Gold, Silver and Bronze” levels of access. Ed Whitacre, chairman and CEO of AT&T said “Why should they be allowed to use my pipes? The Internet can’t be free in that sense, because we and the cable companies have made an investment, and for a Google or Yahoo! or Vonage or anybody to expect to use these pipes [for] free is nuts!”⁴³

To facilitate traditional network based quality control and preferential transmission, technology companies implement Layer 7⁴⁴ packet inspection⁴⁵ and routing based on artificial bottlenecks. This realistically involves breaking the seal on users traffic to examine the packet for the application signature or corraling traffic into junctures to route traffic like a leaky bucket.⁴⁶ It intrudes upon the privacy protections enshrined in the Constitution and the Commons model for the Internet. As such, its only currently implemented in Corporate LANs and internationally in draconian political regimes.

Abroad, especially in China, Western technology companies have been facilitating networks and

40 In Computer Science, an Ontology is a system or domain containing objects bounded by defined constraints

41 Jeff Chester of Democraticmedia.org estimates \$1million dollars a week is spent by the Telco Cartels to undermine Network Neutrality

42 The Content providers already pay for Internet Access, this “pay for play” extends like a tax to all intervening ISPs

43 Business Week November 2005

44 Layer 7 is the topmost or Application level of the OSI model

45 Sometimes called Quality of Service or QoS, its a longtime Telco battlecry, made irrelevant by the internet speed deployment Arms Race

46 The Leaky Bucket is an accepted routing algorithm

control measures deemed unconstitutional in the US. The Natural/National Monopoly telecommunication companies stagger the rollout of Internet access to force and corral users into Internet cafes where monitoring is easier. The big technology companies are only too willing to find another market for expensive network equipment outside of the foreign markets and corporate LAN. Coincidentally, this same infrastructure allows for greater wiretapping capabilities, traffic is now “fair-game” for intrusive monitoring and that monitoring can facilitate “tiers” or Government intrusion (or demographic profiling/marketing).

Calvin Coolidge campaigned for the US Presidency on a platform that “the Business of Government is Business”. The corollary to this business and legislative advocacy is that corporations can lobby and have their concerns prioritized. The major Telcos have spent \$180 million dollars⁴⁷ in the last 10 years in Washington.⁴⁸ Their reward has been preferential tax cuts to encourage broadband and Internet proliferation.⁴⁹ In essence, any arguments on the philosophical underpinnings to the Net, the argument of building intelligence into the network vs relying on the devices connected to the network to provide the intelligence or the nature of privacy protection on the Internet are all moot when its “their” network and the user is not consulted.

Ed Whitacre's⁵⁰ comment is sophistry. Without the content providers, “his” network is useless and worse again, contributes to exaggerating Internet problems not solving them.⁵¹ He offers no concrete evidence that his proposals will facilitate enhanced access for users. His argument that the current generation Internet is insufficient to support future convergence argues more for the abuses perpetrated by the Telcos broadband rollout than the evidence presented by the Peer to Peer companies legislated

47 More than any other Lobby Group

48 Teletruth.com

49 Teletruth.coms Bruce Kushnick estimates the National Internet Alliance/Broadband windfall at \$200 Billion dollars

50 CEO of AT&T

51 AT&T again relays on the Safe Harbour concept to argue against AT&T measures preventing the proliferation of end-user zombies, virus, worm and bot-infected machines

out of existence for providing those same services.⁵² Whitacre's proposal is to punish Internet companies for their success. Companies which rely on the Internet and have no alternate storefront, the “Long Tail” Mom n' Pop stores, Amazon and eBay, the Game Companies, even the gigantic security patches pushed by the big software vendors have no place in AT&T's plans.⁵³

Bill Clinton said in 1998⁵⁴ that governing the Internet was like “nailing jello to the wall”. This was before the Great Firewall,⁵⁵ the Great Sand Curtain⁵⁶ and its equivalents were implemented with the collusion of Western Technology companies. Post 9-11, the Government and the Telcos are desperately trying to justify increased access but for opposing reasons.⁵⁷ My argument is that in conceding to the demands of lobby-heavy AT&T for a preferential Internet access, we will also be forced to abandon the foundations of Internet legislation. I propose a different defense to the “Tiered Internet.” I argue that in increasing the capabilities of the harbour authorities should come a reversal of the Internet legislation which provides safe-harbour provisions which protect unregulated providers.

The Safe Harbour concept that carriers are protected from the misbehavior of their clients is based on there being no way, technically or Constitutionally, for them to intrude into the data stream. When Yahoo hosts Supremacist chat groups, eBay hosts Nazi memorabilia auctions and Verizon does not care, does this criteria apply in a tiered Internet? The tiering of the internet involves intruding upon the privacy of the datastream, where do we draw the line? Layer-7 filtering will break the chain of trust beyond the packet header, its equivalent to the Postal Service opening and reading your letters and routing the mail to a vacationing addressee. Can we protect the I.S.P, the Postal Service, when they are aware of infringing content? The answer, is, of course, **no**. If they are cogniscent of illegality, they have

52 Grokster and Napster provided movies and music on demand on yesterday Internet.

53 Googles response was to threaten to wire America

54 Clinton was giving a speech on Chinese censorship of the Internet.

55 Chinese people access the net under severe censorship and the threat of oppressive monitoring

56 The Saudi Government also imposes strict cultural censorship on its Internet populace

57 The irony is that the US government pays services/providers (Anonymizer) to free/unregulate international Internet surfers from increased level of intrusion internationally.

to report it to the proper authorities.

The Conclusion

The Internet hosts ⁵⁸ a delicate biology of content and interaction ⁵⁹ subject to business and Governmental interaction. The growth of the Internet has proved to be a ready source for conflict between corporate “standards” and shared resources. ⁶⁰ Balanced between the regulation of the Commons and tensions with creeping corporitization is the user and their associated privacy. Your privacy is already subject to unregulated collation, the big Telecommunication companies just want the government to allow them further access, purely for their financial gain. This level of access will be in breach of Constitutional privacy protections.

It is my opinion that Government is engineered to favour Business over the individual. I believe that Constitutional protections against privacy intrusions on the Internet will be reversed to facilitate Corporate and Governmental oversight and intrusion. However, I argue that with this increased input should come a degree of responsibility for the content and any associated legislative infringement. I counter the Telco's greediness with the suggestion “Be Careful what you Ask for”.

⁵⁸ Benklers 3 modes of Communication

⁵⁹ Zittrains theory of “Generativity”

⁶⁰ Lessigs modes of Control