Neo-Luddism and the Demonisation of Technology: Cultural Collision on the Information Superhighway

Don Bowman
Sandvine Incorporated
Waterloo, Ontario, Canada
don@sandvine.com

This article is an editorial note submitted to CCR. It has NOT been peer reviewed. The author takes full responsibility for this article’s technical content. Comments can be posted through CCR Online.

ABSTRACT
The Internet is a primary engine of innovation, communication, and entertainment in our society. It is used by diverse and potentially conflicting interests. When these interests collide in the form of technology, should the Internet stay true to its roots and let things take their course naturally, or should regulation and legislation be enacted to control what may or may not be done. This author believes public opinion is best served by light regulation and a strong focus on allowing technological innovation to take its natural course.

Categories and Subject Descriptors
C.2.3 [Network Operations]: Network management.

General Terms
Human Factors, Economics, Legal Aspects

Keywords
Privacy, network neutrality, network security, network quality of service, quality of experience

1. INTRODUCTION
Few technologies inflame the passions like the Internet. Beginning with its early days as an educational network the Internet has been a technocracy and anarchy, a place where free thinkers could become free doers. In the early days the concept of the consumer Internet did not exist, nor did the concept of an Internet service provider. As the consumer Internet started to grow out of its walled-gardens of early providers like AOL and CompuServe, there was a significant elitist attitude amongst Internet users who attached to it via research organizations [1]. These frictions of cultures, the technocrats versus the newbies, fanned many flame wars, but ultimately lead to many new and innovative technologies to service the needs of these less technical individuals. Technologies such as Gopher, WAIS, and the WWW were all spawned by a desire to make the Internet more accessible to the masses. Many fought the introduction of these new technologies, and typically lesser capable technologies died off, but in the end innovation won out.

Just as the melding of cultures of academics and consumers was becoming stable the Internet came to the attention of bureaucrats and governments. The Internet crossed every boundary imaginable, allowing a server in one jurisdiction to host content for a person in another jurisdiction which was accessed by a third, using wires that travelled through hundreds. Should the Internet be legislated? Taxed? These questions became public policy points. As a global institution, there is no central legal mandate for the Internet. It is run as a loose affiliation of organizations with common goals centering on technology and access. The Internet Engineering Task Force (IETF), the Internet Architecture Board, the IEEE, the major service providers and governments all join forces, and amazingly, it works. Complex protocols like the Border Gateway Protocol (BGP) [2] were designed and built by people who came together with common technology goals, who analyzed problems on their merit rather than their emotions. Government organizations which have not been able to agree on a common two-prong AC outlet were swept by the wayside, and standards were created on technical merit. Some standards, e.g. RFC 1436 (Gopher) [3] came and went as newer, better standards eclipsed them. Speed of innovation and technical merit were the key success factors.

Even later to the game of the Internet than governmental organizations were the big content companies. Media companies fought tooth and nail to prevent their content from being shared online, while hedging their bets with content portals. It was not until recently that business models based on anything other than denial have been tried. Starting in 2009 Apple has started to offer for sale music without digital rights management [4]. NBC, Fox, ABC have banded together to create Hulu, which offers television shows online for streaming. The majority of the media companies still treat the Internet as a vehicle for theft rather than a vehicle for distribution. Media companies spend a lot of money on lobbyists trying to pass legislation preventing sharing of content. It has been 10 years since Napster [5] launched in June of 1999, and the recording industry is still fighting innovation and technology.

Into this virtual realm of real differences of opinion and objectives comes a set of technologies which enables control of what was once considered uncontrollable. Technologies for network policy control allow management of access, quality of service, and bandwidth. This makes people very nervous, fearing it will be used for censorship, or for unfair competition. Network neutrality as a movement was spawned with a goal of preventing restrictions on access of content or modes of communication on residential consumer networks. Strong forces are taking this concept in many directions, and it is a very passionately debated topic, from study halls to halls of government. Many believe that the time is now to move away from an unregulated Internet driven by technical goals and instead restrict the use of these policy enforcement technologies such as the ones made by my company, Sandvine.

Should the Internet remain a technocracy, allowing any and all technologies to be tried, and moving innovation forward without regard to consequences? Should it be regulated and controlled, if so by whom?
2. THE CULTURES OF THE INTERNET

Derogatively referred to as the “Eternal September” [1], America Online (AOL) began offering Usenet access to its members in 1993. This as much as anything marked an end of the era of the Internet as an elite network of academics.

The Internet had always fostered open discussion of opposing viewpoints. Usenet had many controversial groups, and there was no control over starting new ones. Alt.sex was probably the first open electronic forum on sexuality in history, and it was nowhere near the most controversial on in terms of content.

Although initially a North American construct, the Internet quickly became global. Cultures joined with differing languages, differing laws, and differing views on social conditions. The Internet became an experiment in globalism seemingly overnight. Many flame wars were spawned over non-English posts to groups.

The Internet also became a great leveler. Companies with 10 employees can have the same presence as companies with 10 000. Fortunes were won and lost at a fast pace as a communications bubble formed in 1999. Companies wrestled with how to control their image online, how to be noticed online. The corporate culture of the Internet clashed with the personal freedoms of the Internet.

Each group using the Internet has strong opinions and objectives that mirror their real-world façade. They are not neutral. Music fans feel every bit as strongly about their ‘right’ to share music online as the recording companies feel about their ‘right’ to control the distribution. These fundamentally opposing rights sometimes take conflict from the communications world to the real world, involving courts and laws. Freedom of expression, near absolute on the Internet, gives each group an uneducated open forum to make their case. These diametrically opposing views proliferate through many different groups, and these groups often seek technology to favor their message or disfavor their competitors. In [22], the authors believe that these opposing views (the ‘tussle’) are crucial to the architecture and evolution of the network, and need to be accommodated technically.

3. LEGISLATION AND GOVERNMENT

Governmental organizations have traditionally ignored the Internet. Early governmental funding was provided for research purposes, and with the popularization of the consumer Internet, governments were only tangentially involved. Periodically special interest groups would lobby governments on behalf of some freedom which was over or under expressed. Most world governments adopted Internet policy statements which expressed broad goals but affected little regulation. One exception to this was an attempt to prevent monopolies from forming. In many jurisdictions, governments enacted laws or policies that required the incumbent telecom provider to allow third-party Internet providers to use the copper twisted pair phone lines. One can debate the effect of these policies and the reasons behind them, but they were competition typically comes from an alternate technology.

Governments are now taking a more active role. In some jurisdictions such as Australia [7], the government has enacted a policy to force all Internet service providers to do mandatory content filtering. The specter of Government censorship goes against many of the founding principles of Internet access, and it is causing significant conflict. In other countries such as Canada, United States, and the United Kingdom, non-legislative means are being used to cause Internet service providers to subscribe to, and block sites on, a blacklist. In the United Kingdom, the Internet Watch Foundation [9] famously caused Wikipedia to be blocked for editing in the UK when a specific article (that on the band ‘Scorpions’) was placed on the list [8]. Collateral damage is often the result of legislative involvement in technology.

Governments typically get involved when there is a perceived need to protect individuals in society. This protection might be related to a perceived lack of access, enacting policies to increase competition. It might relate to enforcing existing laws in new media, such as the United States “Truth In Domain Names Act of 2003” [12] which seeks to protect children from being tricked into viewing obscenity.

Despite the best of intentions, however, consumers are ill-served by a patchwork of legislation or policy that spans jurisdictions. These policies may be contradictory (for example a local policy which requires pornography-censors in public library access terminals coupled with a regional policy prohibiting censorship in libraries). These policies may also prove a significant barrier to innovation or to doing business for companies which span multiple jurisdictions.

4. MEDIA AND THE INTERNET

Perhaps stronger than any other force in its desire to regulate and control the Internet are the media companies. It is their lobbying efforts and monies which drive legislation such as the United States Digital Millennium Copyright Act (DMCA) [18], and the desire to get a ‘three strikes’ provision added to the EU Telecoms Reform Packages [19] which would force an Internet service provider to permanently disconnect a user who has been found to be distributing copyrighted work three or more times.

While media has a strong desire to control and regulate, it also has a strong desire for innovation. Media companies are slowly learning online distribution, and innovative uses such as Hulu [20]. Media companies drive innovation both in terms of raw delivery speed (bandwidth), but also in terms of quality of service (latency, loss, and jitter). As more and more entertainment shifts to real-time, and as the delivery quality increases, both media companies and consumers benefit [21].

Media companies also, contradictorily, have a strong desire for there to be no control on the Internet, fearing that Internet service providers would use this control to discourage online distribution. Consumer Internet service providers provide an oversubscribed network, and their ability to deliver a quality service to the masses with available technology is challenged by a demographic shift from broadcast medium such as cable-TV to unicast, on-demand medium such as YouTube and Hulu.

5. NETWORK POLICY CONTROL

Network policy control is the enabling technology for many of the best hopes and worst fears of the Internet population. It can give us the quality of service required to stream high-definition video or have crystal-clear voice, but it can also censor or invade our privacy. As a technology it is therefore feared and revered, often by the same people.

Although network policy control encompasses many tools, the single tool which is getting the most attention is deep packet inspection. Deep packet inspection (DPI) is the act of using any field other than the layer-3 destination of an IP packet for any purpose. DPI has been present since the earliest days of the Internet, and is part of technical standards ranging from network address translation application-level gateways (NAT) [13],
through voice over IP (VoIP) session border controllers (SBC) [14]. Practically every consumer home router uses DPI in some way for its functions, to ensure that your file transfer or voice call function, or to ensure that the appropriate priority is given to each packet so that your voice call isn’t interfered with by your file transfer.

DPI also enables other activities that some find objectionable. In the summer of 2008 the United States congress investigated the activities of several Internet service providers and of a company (NebuAd) involved in Internet behavioral advertising [17]. Although no control of the network was envisioned by this use, the US government was concerned about the privacy of the Internet. NebuAd collected the same information that for example Google’s DoubleClick does, but the method of achieving it differed. This investigation more than any other served to demonize the entire class of technologies referred to as DPI.

Network policy control can be used for ‘good’ or for ‘evil’. It is the tool which allows governments to censor access to information on dissident groups. It is also the tool which allows us to transition to IPv6 as we start running out of IPv4 addresses [15]. It is this very control that both excites and worries almost all of the mosaic of cultures which use the Internet. Online media fans see the power of quality of service giving them better experiences, but also see the possibility of censorship.

In the traditional Internet technocracy, this new technology would have found its natural balance. As John Gilmore famously put it, “The Net interprets censorship as damage and routes around it”. [16] As a consequence, when the use of the technology was, on balance better than without, it would have been accepted. When the use was worse, it would have been rejected.

It is precisely this principle which has made the Internet the strong and vibrant force it is today. Rather than demonizing technology with a myriad of uses, we should focus on the good, and discourage the bad, solely based on the merits technically.

6. CONCLUSIONS

Is unfettered Internet access a basic human right? No, the Internet is a technology. It is a powerful tool to improve human rights to be certain. But like all technologies, it will have a rise, a popular period, and perhaps a fall. The use cases span from one technology to another, and will remain after the Internet is gone. Just as one technology (the printing press) enabled a change in course in Western civilization by allowing Luther to get his message out broadly, the technology of the Internet allows this on a daily basis. Just as society did not cry for an end or regulation of the printing press, so too should we not regulate the Internet. Society adapts to changes, adopts technologies that improve it. Attempting to circumvent the natural course of evolution by demonizing a technology, rather than addressing the specific use cases, whether through legislation or the court of public opinion, usually fails.

7. ACKNOWLEDGMENTS

My thanks to all the customers and competitors who have driven the innovations I have observed and the end users of the Internet who have driven the problem domain I have worked in.

I would like to thank the anarchy-that-works in the Wikipedia. This embodies the Internet for me more than any other technology.

I would like to thank my alma mater (University of Waterloo) for introducing me to the wondrous world of Usenet in 1989.

8. REFERENCES