Milton L. Mueller, Syracuse University School of Information Studies, USA

Hadi Asghari, Delft University of Technology, NL

Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States

Two case studies explore the reciprocal influence between technological change and Internet governance. Both focus on the use by Internet service providers of a new capability known as deep packet inspection (DPI) to "throttle" or restrict the speed of BitTorrent uploads or downloads by their customers. We show that in both cases, these implementations led to public protests, litigation and major regulatory proceedings. In both cases, network neutrality norms were used to challenge DPI deployments. The paper's descriptive comparison is supplemented by quantitative data drawn from the use of Glasnost, a network test that allows third parties to detect BitTorrent throttling via DPI.

Introduction

Deep packet inspection (DPI) is a technology for scanning and analyzing Internet traffic and making decisions about how to handle it in real-time. DPI has gained acceptance among many network operators because of its potential to address various Internet governance problems. These include, among other things, the security problems associated with malware (Kim and Lee 2007), copyright protection (Rossenhövel 2008; Beer and Clemmer 2009), and the need to optimize or monetize Internet services (Allot 2007; Vorhaus and Bieberich 2007; Aghasaryan, Kodialam et al. 2010).

Perhaps the most important application of DPI technologies is the power to manage and apportion bandwidth (Coward 2009; Finnie 2009; Mochalski and Schulze 2009). Bandwidth is often a shared, scarce resource on the Internet. The growing number and diversity of Internet applications, especially ones involving video, are increasing the demand for Internet service providers' (ISPs) bandwidth resources. ISPs must invest in its expansion and/or economize on its use. The pressures are especially intense for broadband mobile.

But network management decisions are not just about efficiency; they also involve issues of fairness, privacy and innovation policy. As a tool of bandwidth management, DPI introduces 'intelligence' into what has often been called a 'dumb' network. Data packets are inspected at Layers 2 through 7 as they move through the network, allowing the operator to discriminate among the treatment received by different applications, services or users (Proch and Truesdell 2009). This relatively new capability has the potential to fundamentally alter the politics and economics of the Internet. Classically, the Internet was based on best-effort packet forwarding. The long-running controversy over network neutrality, which is mostly a clash over shifts in the governance of shared bandwidth, is a symptom of the profundity and high stakes of this change. DPI also raises privacy issues by making the network 'aware' of what is going through it, and by linking traffic and content to specific subscribers (Collins 2010; Meyer and Audenhove 2010). It may also undermine or challenge some of the immunities from liability for end user actions that ISPs have traditionally enjoyed (Frieden 2007; Bendrath and Mueller 2011). By the same token, congestion and scarcity are real concerns. Network operators can mount a plausible argument that they have both the right and the obligation to manage their capacity, in which they must place large, risky investments, so as to maintain their profits and optimize customer service (Yoo 2006).

Technology-Society Co-production: Study Method

This paper is part of a larger research project that attempts to systematically analyze the relationship between a change in network technology and changes in the way the Internet is regulated and governed.[1] DPI implies a greatly enhanced capacity to monitor and manipulate Internet traffic, which creates a broad *potential* to dramatically change the architecture, governance and use of the Internet. But it is also possible

[1] Funding support was provided by the National Science Foundation, SBER Division Program on Science, Technology and Society, Award Number: SES-1026916, Milton Mueller, PI.

that DPI will be regulated and limited in ways that will make it consistent with the principles and norms of the existing Internet, or even that certain applications of it will be banned.

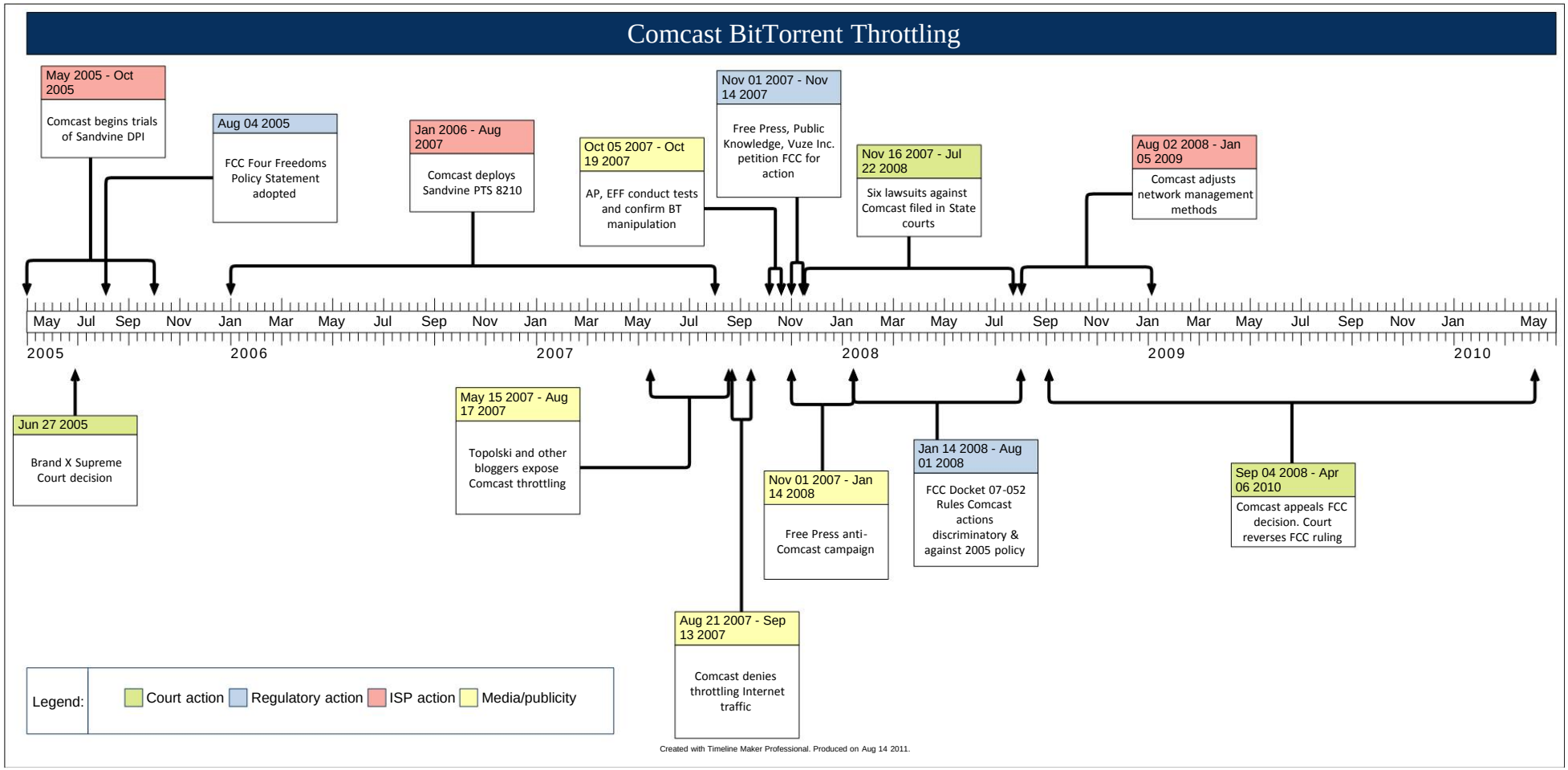
In our view, technological changes do not *determine* social interactions, but neither is technology a passive dependent variable defined entirely by 'social shaping.' The distinctive effects of technologies reflect their unique capabilities, but only insofar as those capabilities serve the interests of specific actors, in specific actor constellations, structured by specific institutional arrangements. We use a framework based on Actor-Centered Institutionalism to analyze these political and market interactions (Bendrath and Mueller 2011). This approach focuses on the *co-production* of technology and governance. The theory of technology/society co-production suggests that 'artifacts and their properties should be analysed neither as objective facts nor as mere social constructions, but as *both* real and constructed' (Brey, 2005). The framework employed in this paper attempts to flesh out that insight by linking the deployment of DPI technology to specific actor constellations, modes of interaction and institutional settings.

A new data source

Empirically, this study develops an extended comparison between two politically-charged uses of DPI for bandwidth management, one in the United States and the other in Canada. In the process of constructing this comparison, we were able to draw on quantitative measures of the use of DPI. A network test known as *Glasnost* was developed by German researchers to detect blocking or throttling of BitTorrent and other peer to peer (P2P) file sharing protocols. The detailed workings of the Glasnost test are described in Dischinger, Marcon, et al (2010). Thanks to an initiative known as the Measurement Lab[2] (MLab), supported by Google and the New America Foundation's Open Technology Initiative, the Glasnost test was placed on a global platform so that end users all over the world could run the test and the results would be stored and made available to researchers. This way of crowdsourcing the generation of network performance data provided the researchers with data for the last three quarters of 2008, all of 2009 and the first quarter of 2010. An Internet user who runs the Glasnost test can see whether BitTorrent is completely blocked, slowed down (throttled) or running normally. (ISPs who block or throttle BitTorrent almost always do the same to other P2P protocols, although the policies applied may differ.)

This study begins with narratives describing the institutional setting in each country, the implementation of DPI by providers, the process by which it became politicized, and the legal and regulatory proceedings and decisions leading to a governance outcome. We then show how these events were reflected in the Glasnost data. We find a counter-intuitive result – what we call the network neutrality paradox - that raises some interesting questions about regulation and legal protections.

[2] http://www.measurementlab.net


Comcast BitTorrent Throttling
May 2005 - Oct 2005
Comcast begins trials of Sandvine DPI
Aug 04 2005
FCC Four Freedoms Policy Statement adopted
Jan 2006 - Aug 2007
Comcast deploys Sandvine PTS 8210
Oct 05 2007 - Oct 19 2007
AP, EFF conduct tests and confirm BT manipulation
Nov 01 2007 - Nov 14 2007
Free Press, Public Knowledge, Vuze Inc. petition FCC for action
Nov 16 2007 - Jul 22 2008
Six lawsuits against Comcast filed in State courts
Aug 02 2008 - Jan 05 2009
Comcast adjusts network management methods
May Jul Sep Nov Jan Mar May Jul Sep Nov Jan Mar May Jul Sep Nov Jan Mar May Jul Sep Nov Jan Mar May Jul Sep Nov Jan May
2005 2006 2007 2008 2009 2010
Jun 27 2005
Brand X Supreme Court decision
May 15 2007 - Aug 17 2007
Topolski and other bloggers expose Comcast throttling
Nov 01 2007 - Jan 14 2008
Free Press anti-Comcast campaign
Jan 14 2008 - Aug 01 2008
FCC Docket 07-052 Rules Comcast actions discriminatory & against 2005 policy
Sep 04 2008 - Apr 06 2010
Comcast appeals FCC decision. Court reverses FCC ruling
Aug 21 2007 - Sep 13 2007
Comcast denies throttling Internet traffic
Legend:
Court action
Regulatory action
ISP action
Media/publicity
Created with Timeline Maker Professional. Produced on Aug 14 2011.

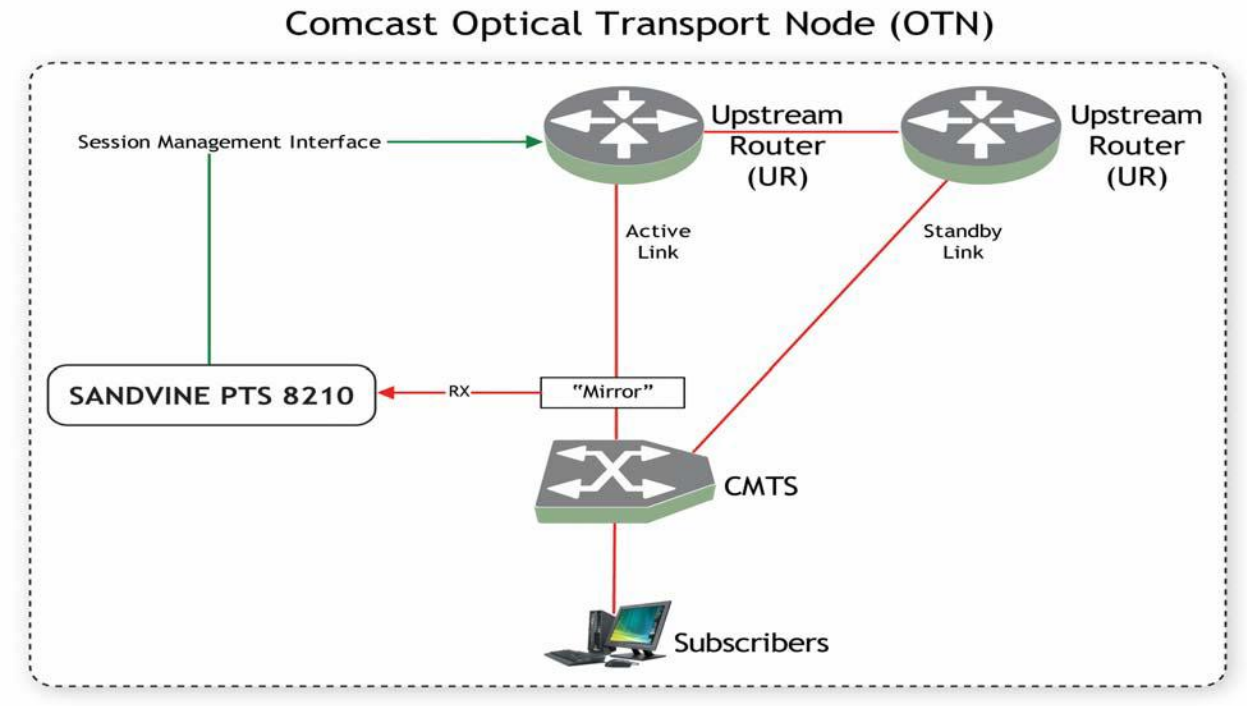
USA: The Comcast case

The timeline page (Figure 1) maps out the events in the U.S. that were triggered by Comcast's deployment of DPI to interfere with BitTorrent traffic. There was a unilateral initiative by Comcast to conduct trials of DPI to analyze its traffic beginning in May 2005. Shortly afterwards, the U.S. Supreme Court upheld the FCC's classification of cable modem ISPs as deregulated "information service" providers, which likely reinforced Comcast's management's belief that they could deploy the technology without permission or notification.

Deployment and public exposure

Deployment began in January 2006 and spread throughout its networks for the next 18 months. Comcast's implementation architecture is diagrammed in Figure 2. From May to August of 2007, technically well-informed users of its service began to notice and publicize the effects of the deployment. Robb Topolski, writing on *DSL Reports* in May, was probably the first, but a blog post on TorrentFreak in August seemed to have catalyzed the strongest reaction. Though Comcast publicly denied interfering with BitTorrent, tests and reports by the Associated Press and EFF confirmed Topolski's analysis.

Figure 2



While Comcast's DPI implementation potentially limited or disrupted the type of service its customers would receive, the change took place without any notice to its customers or any alteration of their service contracts. After these practices were exposed, Comcast web sites began to refer to procedures

for "managing" P2P traffic, but referred to its measures as "delaying" the traffic when in reality the effect was usually to block it.

The FCC Proceeding

On November 1, 2007, public interest groups Free Press, Public Knowledge and a group of law professors filed a complaint with the FCC, viewing this as a critical test case for the network neutrality cause. Two weeks later, a similar petition was filed by a commercial entity which was attempting to develop an "open entertainment platform" business using P2P software to distribute video content to Internet users, Vuze Inc.[3]

Free Press then launched a public mobilization against Comcast which generated 22,284 emailed complaints to the FCC over the next two and a half months. But that was not the only backlash. From mid-November 2007 to the middle of June 2008, civil actions were filed in at least six State courts.[4] The lawsuits typically charged Comcast with false advertising for claiming to offer high speed service while deliberately interfering with access speeds. Some suits also charged that Comcast was violating federal policy, citing the FCC's 2005 Policy Statement.

The FCC on 14 January 2008 consolidated the Free Press and Vuze petitions into a single proceeding and formally issued a call for public comment.[5] Between February and July 2008 over 6,500 comments were received, an unusually large number for an FCC proceeding. In addition to requesting written comments, the FCC held a series of public hearings around the country to provide an opportunity for face to face testimony from local constituencies.

The FCC decision on August 1, 2008 concluded that Comcast's practices were discriminatory and did not constitute reasonable network management.[6] Comcast was also judged guilty of a failure to disclose its practices to its users. The two Democrats on the Commission joined Republican Chairman Kevin Martin in a 3-2 majority. In asserting its authority to make these determinations, the Commission relied heavily on a 2005 Policy Statement based on then-Chairman Powell's notion of the "four freedoms" of Internet users. The FCC claimed that it could enforce the statement using its "ancillary" jurisdiction under Title I. Comcast's counter-arguments had asserted that the FCC had no authority to regulate its network management practices.

---

[3] Broadband Industry Practices, WC Docket No. 07-52, Petition to Establish Rules Governing Network Management Practices by Broadband Network Operators of Vuze, Inc., (Nov. 14, 2007)

[4] Hart v. Comcast, No. 07-6350 (N.D. Cal.); Leigh v. Comcast, No. 08-4601 (C.D. Cal.); Lis v. Comcast, No. 08-3984 (N.D. Ill.); Libonati v. Comcast, No. 08-3518 (D.N.J.); Topolski v. Comcast, No. 08-852 (D. Ore.); Tan v. Comcast, No. 08-2735 (E.D. Pa.).

[5] Broadband Industry Practices, WC Docket No. 07-52, Comment Sought on Petition for Declaratory Ruling Regarding Internet Management Policies, Public Notice, 23 FCC Rcd 340 (WCB 2008); Broadband Industry Practices, WC Docket No. 07-52, Comment Sought on Petition for Rulemaking to Establish Rules Governing Network Management Practices by Broadband Network Operators, 23 FCC Rcd 343 (WCB 2008).

[6] FCC-08-183, WC Docket No. 07-52 Adopted Aug 1 2008, Released Aug 20, 2008

The remedy mandated by the August 2008 decision ordered Comcast to stop using its current method of P2P blocking and to develop new ones that were "protocol-agnostic;" i.e., did not discriminate against particular applications or protocols. It was also ordered to disclose the technical details of the DPI methods it had used.

Despite the drama of the August 2008 FCC decision, the most important outcome had already occurred months earlier. Faced with the avalanche of negative publicity, litigation, and the threat of regulatory action, Comcast on March 27, 2008 had already offered the FCC a "voluntary agreement" to alter its reviled P2P blocking practices.[7] Also, it eventually agreed to settle one of the state-level class action lawsuits for $16 million.[8]

Comcast's new bandwidth management methods, described in a September 19, 2008 filing at the FCC, would no longer single out P2P protocols in general or BitTorrent in particular for disruption or throttling. Instead, the system would only check for congestion thresholds in geographically delimited network segments at 15-minute intervals.[9] If congestion existed, regardless of the applications used, the intelligence built into the network would identify which specific customers were contributing the most to the traffic flows. Those customers' packets would be de-prioritized during the ensuing 15 minute cycle. This new method used DPI equipment, but only for traffic monitoring and the linking of specific customers to high-volume traffic flows. It did not inspect the contents of the packets.

Comcast began trials of its new methods in August 2008. It also announced a new acceptable use policy (AUP) establishing a monthly data cap of 250 GB per month per account for all residential customers which would go into effect October 1, 2008. On January 5, 2009, Comcast issued a letter to the FCC confirming its transition to the new application-neutral procedures.[10]

Even as it complied with the FCC's ruling, Comcast appealed the FCC decision to the D.C. Circuit court. While it had complied with the norms of the mobilized community and the order of the regulatory agency, Comcast was clearly intent upon contesting the agency's authority to regulate their network management practices. The FCC on the other hand moved even further toward support for network neutrality. The election of Barack Obama as President gave Democrats the chairmanship of the Commission and a secure voting majority. By October 2009 the new administration's FCC had developed a Notice of Proposed Rulemaking (NPRM) that would create new industry-wide rules it claimed would safeguard network neutrality.[11]

---

[7] Ex Parte Letter of David L. Cohen, Comcast Corp., to Chairman Kevin J. Martin et al., FCC, WC Docket No. 07-52 (Mar. 27, 2008).
[8] Hart v. Comcast, United States District Court for the Eastern District of Pennsylvania. http://www.p2pcongestionsettlement.com/
[9] September 19 2008 Comcast filing.
[10] Ex Parte Letter from Kathryn A. Zachem, Comcast Corp., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 07-52, File No. EB-08-IH-1518 (Jan. 5, 2009).
[11] FCC 09-93

The FCC overturned

Comcast won its appeal of the August 1 FCC decision. The Court held that the FCC lacked the authority to order Comcast to change its network management processes.[12] The ruling completely disrupted the trajectory that FCC network neutrality policy had taken since the passage of the Powell Policy Statement five years earlier. The two main options facing the FCC both seemed bleak. It could accept the status quo, or it could generate a massive political battle by seeking new legislation from Congress and/or by reversing its own 2002 ruling that cable modem Internet service providers are 'information services' and re-classify them as 'telecommunication services' regulated as common carriers.

The FCC eventually chose what it called a "third way." This involved a limited reclassification of only the "transmission component" of Internet service as telecommunications and a decision to forbear from applying all of the relevant sections of the Communication Act to broadband Internet.[13] The FCC's "Open Internet" rulemaking went through several rounds of comment and revision and by December 22, 2010, the Democrat majority succeeded in passing the new rules. But at the time of this writing, the capture of Congress by the Republicans in the 2010 elections meant that Congress was likely to attack and reverse the new rules, and they are already being challenged in court.

Thus in the United States, DPI's deployment for bandwidth management purposes destabilized the political and regulatory equilibrium around Internet governance. Yet at the same time the political and market pressures associated with the controversy succeeded in seriously constraining DPI's use.

Canada: From P2P throttling to Usage-based Billing

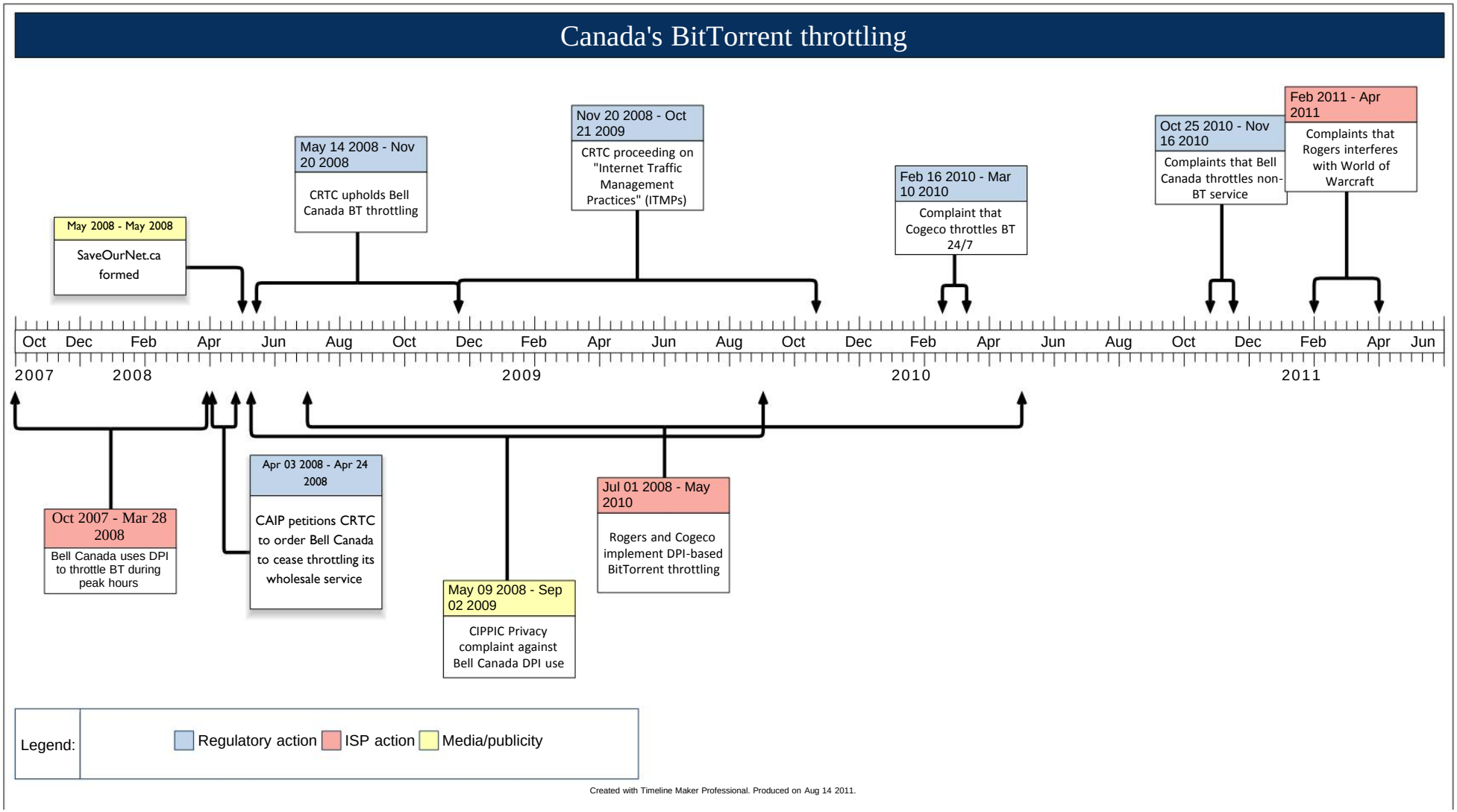
The timeline (Figure 3) summarizes how developments played out in Canada. Canada's institutional setting is similar in some respects to that of the United States. It is a federal system and its federal regulator, the Canadian Radio-Television and Telecommunications Commission (CRTC), has a scope of authority that closely parallels that of the United States' FCC. But there are two key differences. One is that Canada's Telecommunications Act does not exempt facilities-based broadband Internet service providers from common carrier regulation. Section 36 of its Telecommunications Act protects Canadian Internet users' ability to access and use legal Internet content and applications of their choice. Section 27(2) effectively protects Internet content and application providers' ability to reach users without discrimination or preference from the regulated carrier (McTaggart 2008).

---

[12] Comcast v. FCC; NBCU intervenors; US Court of Appeals for the DC circuit decision. Argued Jan 8, 2010, Decided Apr 6, 2010. The FCC's argument is "flatly inconsistent with Southwestern Cable, Midwest Video I, Midwest Video II, and NARUC II, but if accepted it would virtually free the Commission from its congressional tether." 440 U.S. at 706.

[13] The new approach was outlined in Julius Genachowski (Chairman), "The Third Way: A Narrowly Tailored Broadband Framework," Federal Communications Commission, May 6, 2010.

Canada's BitTorrent throttling



Another important institutional difference is that Canada requires its larger, facilities-based Internet service providers, Bell Canada and Rogers, to sell bandwidth at wholesale, regulated rates to competing Internet service providers. This is intended to promote competition by giving smaller firms access to facilities controlled by a dominant incumbent. Bell Canada, the former telephone monopoly, is the main wholesale Internet access provider regulated by the CRTC.[14] The unbundling of wholesale and retail access alters the actor constellation by creating a class of smaller, 'retail' ISPs who are stakeholders in the regulations applied to Bell Canada.

Yet another institutional difference is that Canada has stronger federal data protection laws than the U.S., and a national Privacy Commissioner. Thus while there was no organized network neutrality movement (one developed later), there was an active and professional community of privacy and civil liberties groups who initially framed the struggle over DPI and bandwidth management as a privacy issue.

DPI deployment in Canada

As in the U.S., DPI deployments initially targeted P2P protocols. But the implementations and policies differed across providers, as one would expect from a pattern of uncoordinated, unilateral deployment by individual providers.

Although it is possible that Shaw had deployed DPI earlier, the controversy arose when Canada's largest provider, Bell Canada, decided that DPI should be used to deal with Internet congestion.[15] In October 2007 it started using DPI to control the use of P2P protocols by users of its retail Internet service, Sympatico. Bell's implementation slowed down both the upload and download rates of all P2P file-sharing applications, but only from 4:30 p.m. to 2:00 a.m. Prior to March 2008, the cable networks' and Bell Canada's use of DPI was generating a small but growing chorus of complaints from regular users of P2P applications. As in the U.S., consumers who had purchased what they thought were unlimited service packages at high speeds felt cheated when their use of BitTorrent was slowed to dial up rates.[16]

After several months Bell management decided that retail-level throttling did not adequately address congestion problems. Indeed, the wholesale-retail split posed an interesting dilemma for Bell Canada. If it rate-limited its own retail customers and left its wholesale facilities untouched, then congestion might still exist, and users of their wholesale competitors would be de facto prioritized on the wire. Since the ostensible purpose was to reduce congestion, the extra bandwidth conserved from their own users would shift to the wholesale ones. Near the end of March 2008 it began to apply

---

[14] A 1999 CRTC Telecom Order (99-592) concluded that the retail Internet service market was sufficiently competitive to protect users without regulation. The CRTC thus forbears from regulation of retail Internet services, but does not forbear from regulating the services that primary ISPs provide to secondary ISPs.

[15] Response to interrogatory The Companies (CRTC)4 Dec08-8 a) and b).

[16] "Bell Sympatico P2P Black List" P2PNet.Net, November 3, 2007. http://www.p2pnet.net/story/13883.

the same pattern of P2P rate-limiting to its wholesale Gateway Access Service (GAS).

Regulatory Proceeding against Bell Canada

Once DPI-based BitTorrent throttling was applied to wholesale GAS, smaller retail ISPs could not offer customers a service without such throttling. Thus on 3 April 2008 their trade association – the Canadian Association of Internet Providers (CAIP) – filed papers asking the CRTC to direct Bell Canada to cease and desist from throttling Internet traffic generated by P2P file-sharing applications. CAIP argued that Bell Canada's GAS tariff did not allow traffic shaping, and so by unilaterally applying traffic shaping to its GAS customers, Bell Canada had altered the terms of its service without prior approval by the Commission.

Starting in May 2008, the Canadian proceeding coincided with the middle of the widely-publicized Comcast proceeding in the U.S., so the Canadian environment could easily pick up on network neutrality framing and norms. Citizens groups mobilized to support the CAIP petition and framed the issue along network neutrality lines. A new public interest coalition was organized in May 2008, known as SaveOurNet.ca. Like the U.S. Comcast proceeding, the Bell Canada/GAS proceeding attracted large numbers of public comments, involving 1,300 individuals and organizations.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) joined in the attack. On May 9 2008 it filed a complaint with the Privacy Commissioner claiming that Bell's use of DPI for network management violated the nation's privacy law because of its "unnecessary and non-consensual collection and use of personal information."[17]

The CAIP/Bell Canada proceeding sparked a sophisticated debate over the appropriate rules and principles to govern shared bandwidth. Bell Canada defended its actions by noting that a small proportion of users were generating a disproportionate amount of network traffic and a significant amount of that traffic was attributable to P2P applications. In Bell Canada's view, such usage degraded the Internet service of other users by creating congestion.[18] Cable operator Rogers supported Bell Canada's position, as did Cisco Systems, a vendor of DPI equipment. Cisco claimed that P2P applications were configured to eat up any additional bandwidth the company added.

CAIP and others disputed Bell Canada's definition of congestion and its method for measuring it. They denied that P2P applications are more bandwidth-hungry than any other application. CAIP argued that Bell's DPI implementation filtered non-P2P protocols, claiming that users who start P2P clients were 'flagged' and once this happened other applications, such as

---

[17] The CIPPIC complaint is available at http://www.cippic.ca/uploads/Bell-DPI-PIPEDAcomplaint_09May08.pdf.

[18] Bell Canada pointed to article 8.3 of item 10 (Terms of Service) of its General Tariff, which states: "Customers are prohibited from using Bell Canada's services or permitting them to be used so as to prevent a fair and proportionate use by others. For this purpose, Bell Canada may limit use of its services as necessary."

SSH and VoIP, were slowed down too.[19] More importantly, they argued that Bell's general Terms of Service could not be invoked to authorize systematic traffic shaping on a network-wide basis. The appropriate response to congestion, in their view, would be to limit or terminate service to specific bandwidth hogs, rather than throttling all P2P protocols.

On November 1 2008, the CRTC denied CAIP's application.[20] Bell Canada was victorious on almost every issue raised in the proceeding. The CRTC ruled that Bell Canada did not violate the terms of its GAS tariff; that its traffic shaping did not give it a discriminatory competitive advantage; that Bell did in fact have congestion and capacity issues to solve; that its use of DPI did not illegally modify the content of transmissions; and that DPI use did not by itself violate privacy rights. Bell Canada was lightly slapped on the wrist for not properly giving advance notice to its wholesale customers of its DPI implementation.

That decision, however, did not settle the issue. The CRTC realized that complaints about Bell's use of DPI were turning into a general policy debate over bandwidth management and network neutrality. Along with its adverse decision on the CAIP petition it issued Telecom Public Notice CRTC 2008-19, a proceeding to review "the current and potential Internet traffic management practices of [all] Internet service providers."[21] It accepted written comments until 16 Feb 2009, and scheduled oral hearings for June 2009. It also commissioned an expert report on ISP Traffic Management Technologies, which appeared in January 2009 (Finnie, 2009).

The ITMP Proceeding

The proceeding on Internet Traffic Management Practices (ITMPs) attracted even wider interest than the previous one. The carriers had to provide detail on what kind of ITMPs they were using and whether they used DPI or not. As in the Comcast case, the cause of transparency was advanced, as the underlying practices were exposed and their distributional effects debated and measured against public norms.[22]

Network neutrality advocates from the United States allied with newly-formed coalitions in Canada. In 2009, SaveOurNet.ca held well-attended "Open Internet Town Hall" events in four cities. Over 12,000 citizen comments calling for net neutrality were sent to the CRTC. A broad coalition of civil society groups expressed support for network neutrality norms.

In its final 21 October 2009 decision (Telecom Regulatory Policy 2009-657) the CRTC articulated a "Framework for determining acceptable ITMPs." The CRTC claimed that it had developed "a principled approach that appropriately

---

[19] Nate Anderson, "New filings reveal extent, damage of Bell Canada throttling" Ars Technica, June 2, 2008 http://arstechnica.com/old/content/2008/06/new-filings-reveal-extent-damage-of-bell-canada-throttling.ars

[20] Telecom Decision 2008-108 http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm

[21] Telecom Public Notice CRTC 2008-19 http://www.crtc.gc.ca/eng/archive/2008/pt2008-19.htm

[22] Michael Geist blog, In Case You Missed It: Reflecting on the CRTC's Net Neutrality Hearing, Wednesday July 15, 2009. http://www.michaelgeist.ca/content/view/4135/125/

balances the freedom of Canadians to use the Internet for various purposes with the legitimate interests of ISPs to manage the traffic thus generated on their networks, consistent with…privacy legislation." Its approach was based on four principles: Transparency, Innovation, Clarity and Competitive Neutrality.

1. The *transparency* principle meant that ISPs must disclose their use of ITMPs to consumers, so their customers can make informed decisions. The CRTC praised "economic practices" as "the most transparent form of network management" because "they match consumer usage with willingness to pay, thus putting users in control and allowing market forces to work."

2. The *innovation* principle gave a mixed message. It said that network expansion should be the "primary tool" for dealing with congestion, but recognized that investments in network expansion cannot eliminate the need for ITMPs. Thus it recognized ITMPs as a necessary last resort that must be designed to address a defined need, and nothing more.

3. The *clarity* principle warned ISPs not to use ITMPs that are "unjustly discriminatory" or "unduly preferential." In order to flesh out the meaning of discriminatory network management, the Commission established a detailed framework that provides "a structured approach to evaluating whether existing and future ITMPs are in compliance with the anti-discrimination sections of the Telecommunications Act (subsection 27(2))." The framework prohibited outright blocking of Internet content by the ISP and required that all ITMPs should be disclosed by both primary and secondary ISPs. It said that if an interactive application was purposely slowed, it would constitute an illegal influence on the meaning of communications. But it allowed ISPs to slow down non-interactive applications to achieve a narrow technical goal. On the other hand economic ITMPs – i.e., pricing tiers or metered usage – were broadly endorsed by the CRTC as not "unjustly discriminatory."

4. The *competitive neutrality* principle was intended to prevent ITMPs from being used in a way that would undermine competition. Based on the assumption that retail Internet service is a competitive market, the CRTC allowed ISPs to employ network management technologies in their retail services without prior Commission approval. If consumers complain, the Commission will review the practices, assessing them against the ITMP framework. The CRTC promised additional scrutiny for wholesale services.

On privacy, the CRTC recognized the need to supplement the protections of the Personal Information Protection and Electronic Documents Act (PIPEDA) and "directs all primary ISPs...not to use for other purposes personal information collected for the purposes of traffic management [of retail services] and not to disclose such information." Contracts with secondary ISPs must require same commitment.

The comparison as reflected in Glasnost data

The Glasnost data provides a quantitative measure of DPI use for BitTorrent blocking or throttling. It allows us to see how the percentage of positive

tests changed over time, and to match major changes to external events, such as regulatory decisions, publicity and the like.

Figure 4a: Number of Glasnost tests over time, USA ISPs.

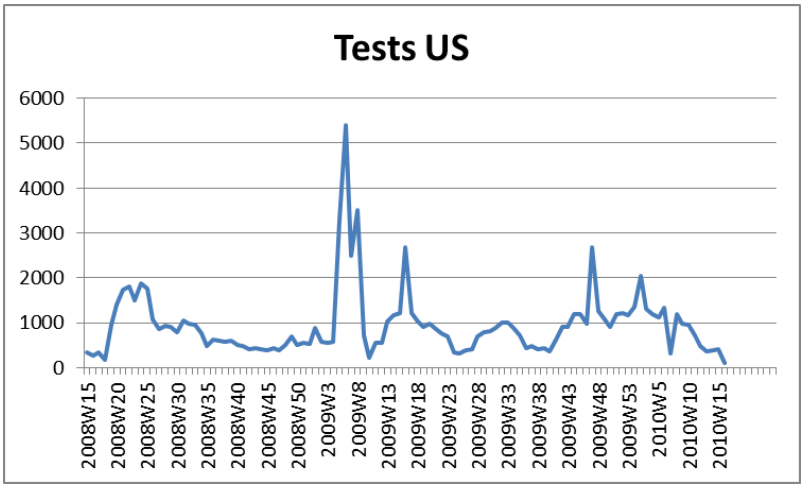
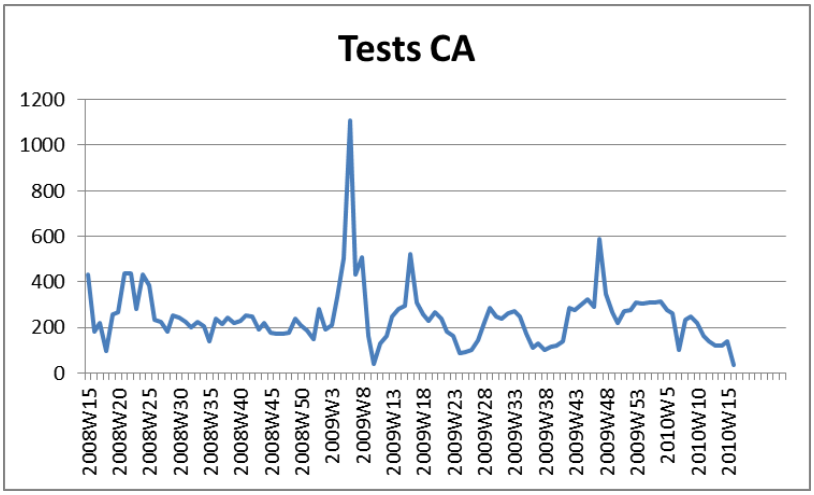


Figure 4b: Number of Glasnost tests over time, Canadian ISPs.



Glasnost is 'crowd-sourced' data; people on the Internet have to choose to run the tests. The graphs in Figure 3 show the number of Glasnost tests that were conducted by users in the U.S. (4a) and Canada (4b). The chart shows variation in the number of tests on a weekly basis from the 15th week of 2008 (April) to the 15th week of 2010. The spike around January 2009 reflects a publicity effort by Google. This date range corresponds fairly well, though not perfectly, with the U.S. FCC's Comcast proceeding (14 January to 1 August 2008) and the network neutrality proceeding afterwards. It also overlaps with the Canadian regulator's Bell Canada DPI proceeding (May 2008 – November 2008) and its ITMP proceeding (November 2008 – October 21, 2009). In the U.S., there are usually over 500 tests per week, often 1000 or more, whereas in Canada the average is around 200 tests per week, occasionally shooting up over 400.

Figure 5: Comcast's use of DPI

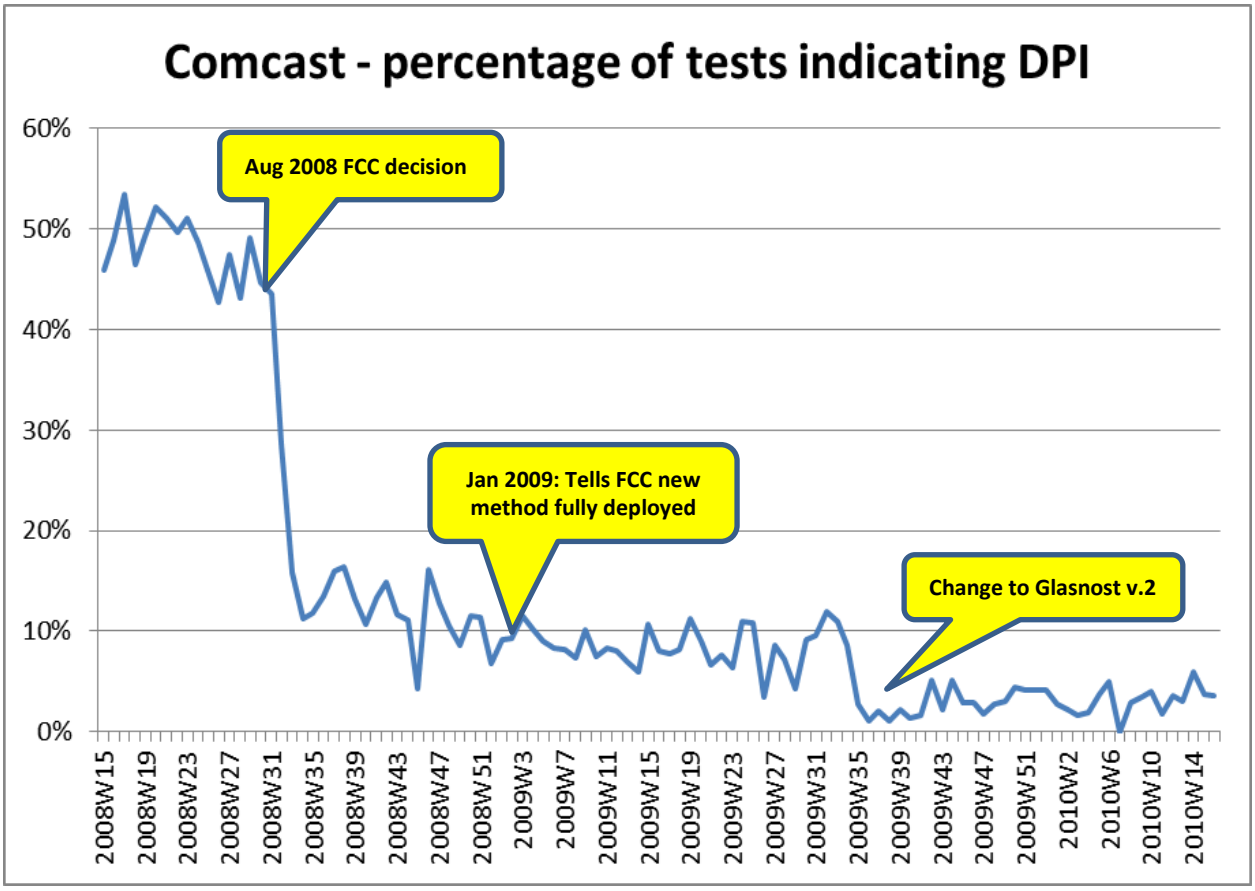
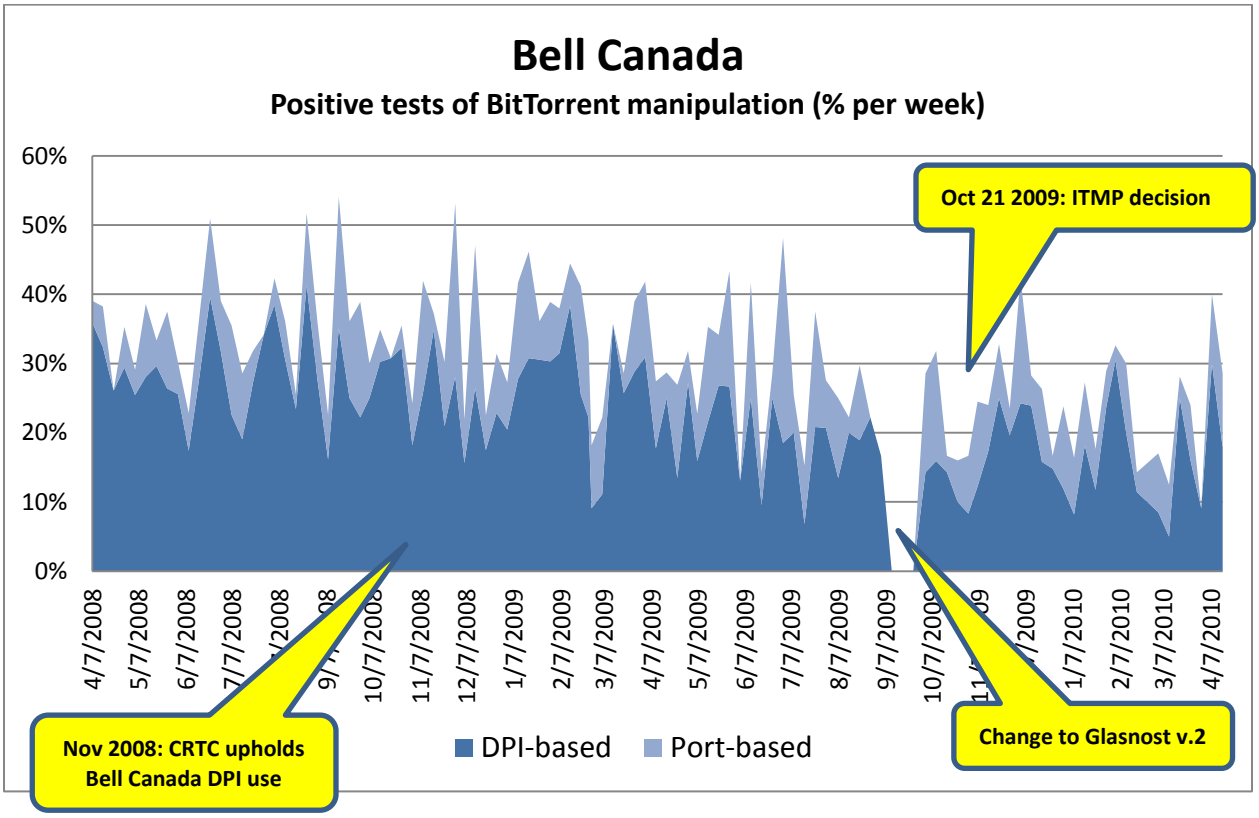


Figure 4 shows the dramatic impact that the FCC proceeding, decided 1 August 2008, had on Comcast's use of DPI to manipulate BitTorrent traffic. Positive identifications plummeted from nearly 50% of all tests to around 10% and from there to a negligible amount (3-5%, possibly measurement error). Figures 5 and 6, on the other hand, show that Canadian ISPs' use of DPI for BitTorrent manipulation was almost completely unaffected by the regulatory proceedings. Bell Canada's throttling stays within the same range (20-40%) before and after the regulatory challenge of May – November 2008. There was a month-long hiatus in the Glasnost results caused by a change in the nature of the test between August 25 and October 8, 2009. The new test is thought to be less noisy and tends to provide slightly lower positive results. Taking that into account, the ITMP ruling of October 21, 2009 seems to have had no discernable impact on positive test results for the rest of the test period, though we need to extend the data.

Intriguingly, the tests reveal that Canada's largest cable operators, Rogers and Cogeco, switched on DPI-based BitTorrent throttling on the exact same date: July 1, 2008. Both operators throttled BitTorrent at all times of day, regardless of congestion. Figure 6 shows that positive tests for Rogers, a larger provider for which there are more tests, hovers around 90-100% until

September 2009. After the change to Glasnost v.2, positive tests are around 80%. The results for Cogeco are far more variable, but this is because there are far fewer tests per week for this smaller cable-modem ISP. Cogeco also shows nearly 100% positive results after July 2008, but its manipulation of BitTorrent seems to decline after January 2010.

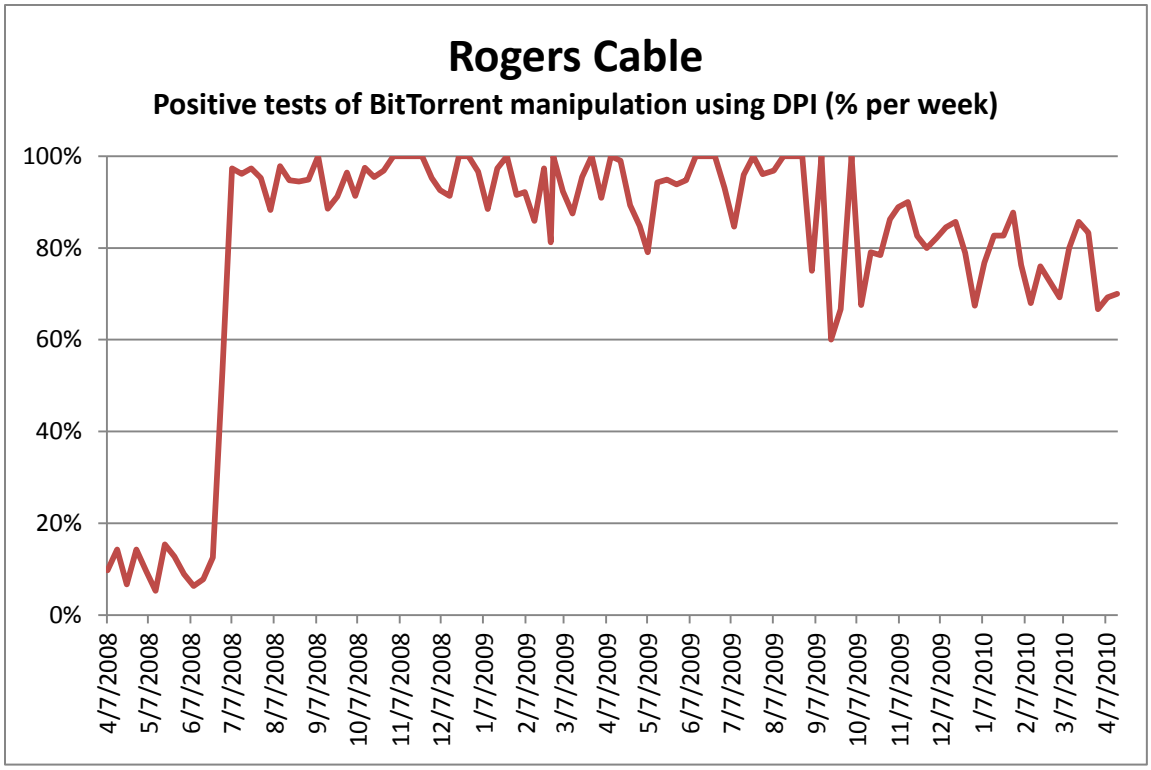
Figure 6: BitTorrent throttling by Bell Canada



Tables 1 and 2 display the data in numerical format disaggregated by ISP and by country. The data reveals the difference that a provider's infrastructure makes in the decision to deploy DPI for bandwidth management. In the U.S. a wireless ISP such as Clearwire and ISPs that rely on cable infrastructure (such as Comcast, Cox and Charter) were much more likely to make major use of DPI for BitTorrent throttling prior to the FCC decision. DSL-based companies in the U.S. show far fewer positive test results. In Canada, cable infrastructures are also more likely to use DPI, but DSL-based provider Bell Canada uses it, while former incumbent Telus seems not to.

Especially notable in Table 2 is that the Comcast controversy seems to have affected the conduct of other cable-infrastructure ISPs in the U.S. Cox, Insight and Charter show major declines in BitTorrent throttling after the FCC decision.

Figure 7: BitTorrent throttling by Rogers & Cogeco Cable, 2008 – 2010



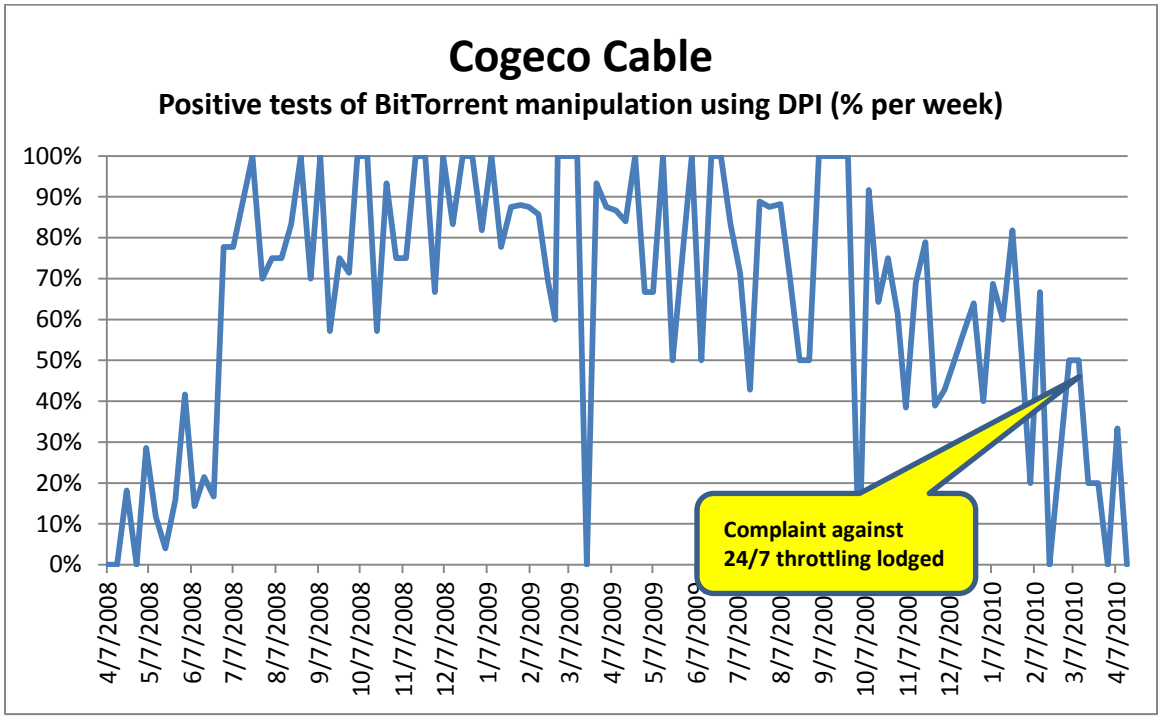


Table 1: Canadian ISPs

Operator	2008H1	2008H2	2009H1	2009H2	2010H1
Bell Aliant	*10%	13%	14%	11%	*6%
Bell Canada	26%	23%	26%	17%	17%
Cogeco Cable	13%	74%	82%	63%	44%
Rogers Communications	8%	82%	91%	81%	78%
SaskTel	0%	7%	10%	6%	5%
Shaw Communications	12%	19%	31%	20%	14%
Telus Communications	6%	10%	6%	5%	6%
Videotron	*5%	*4%	5%	1%	*3%

* - Total number of test results is less than .02% of the number of subscribers

Table 2: US ISPs

Operator	2008H1	2008H2	2009H1	2009H2	2010H1
Comcast	49%	23%	8%	5%	3%
Charter Communications	14%	19%	14%	8%	5%
Cox Communications	52%	30%	8%	4%	3%
Insight Communications	13%	9%	9%	4%	6%
Time Warner Cable	10%	10%	8%	5%	4%
Cablevision Systems	12%	10%	10%	8%	*7%
Clearwire	*27%	*57%	66%	28%	17%
Covad Communications	5%	3%	2%	3%	*7%
Verizon Communications	*7%	*5%	5%	4%	*2%
Windstream Communications	*8%	*2%	6%	6%	*5%
Qwest Communications	*9%	*9%	7%	4%	*7%
AT&T Inc.	9%	10%	8%	5%	4%
CenturyLink	8%	9%	8%	5%	4%

* - Total number of test results is less than .02% of the number of subscribers

On an aggregate basis across all ISPs from April 2008 – April 2010, U.S. ISPs test positive for DPI only 11% of the time, whereas Canadian ISPs test positive 33% of the time. (Such an aggregate view, of course, fails to capture variation in ISP policies, as well as the effect of critical events that affected their usage of DPI, such as the regulatory proceedings.)

Concluding Analysis

In both the United States and Canada, the new technical capabilities of DPI were deployed unilaterally and without public notice or regulatory approvals by major Internet service providers from early 2006 on. The primary purpose was to throttle or block P2P applications to conserve bandwidth. In both cases, adverse or unexpected impacts of its use on some consumers were

discovered shortly after deployment, leading to negative publicity, public mobilizations, litigation and major regulatory proceedings. In both cases, network neutrality norms were used to challenge DPI deployments. In both cases, the regulatory proceeding first focused on DPI use by one major carrier, but then led to more general proceedings focused on the broader questions of legitimate bandwidth management practices and neutrality norms.

But the outcomes differed in a paradoxical way. In Canada, existing law already defined the major ISPs as common carriers and banned them from undue discrimination and from influencing the meaning of communications. Canadian law thus provided exactly the legal framework that U.S. net neutrality advocates craved. Yet the Canadian carriers' traffic shaping practices were upheld and ratified by the regulator. For better or worse, the Canadian process left things unchanged. In the U.S., on the other hand, the use of DPI for network management led to a major public confrontation that changed a lot. From a governance standpoint, the confrontation eviscerated the FCC's authority to regulate ISPs' network management practices.[23] But the uses of DPI by US cable ISPs were dramatically changed nevertheless, and the changes made DPI much more application-neutral and more narrowly targeted on congestion than in Canada. Ironically, the country with no net neutrality law ended up with more net neutrality.

These case studies and quantitative measures corroborate the following general insights:

- DPI is disruptive in Internet governance. It thrusts into the hands of network operators powerful new capabilities to manipulate traffic. The power to shape traffic flows redistributes agency and control among actors in the ecosystem, namely network operators, users, and the service/application providers. This redistribution of agency generates broad political economy debates about efficiency, fairness, innovation and transparency. But the way those conflicts are resolved in regulation and policy depends heavily on the specific actor constellation and institutional setting, and can lead to unpredictable and even paradoxical results.
- Bandwidth management is one of the most important, widespread and controversial applications of DPI. This was not what we expected.[24] The massive growth in the number and variance of services delivered over the Internet gives bandwidth management high economic stakes. The ancillary effects of bandwidth management methods extend into all aspects of the internet economy.
- There seems to be an inexorable trend towards utilizing in-network intelligence to realign usage levels with service pricing. But there are major distributional consequences in *how* this is done. Just how big the distributional effects are can be seen by contrasting the amount of rate-limiting done by Comcast before (~50%) and after (~5%)

[23] The issue of the FCC's authority to regulate is still not fully resolved as of mid-2011.

[24] We expected surveillance, censorship and copyright policing to be more likely to generate political debates and regulatory-institutional change, and that bandwidth management would be a relatively uncontroversial application.

its public exposure and the FCC intervention. It is also evident from the difference between Comcast's congestion-triggered traffic shaping and Rogers Cable's indiscriminate throttling of BitTorrent. These huge differences in throttling levels are likely to have major effects on users and on the functioning of the internet economy.

- An organized network neutrality movement can play and has played a major role in shaping the impact of DPI technology on Internet governance. As a general norm, network neutrality is potent. But…
- Laws and regulations that require common carriage and nondiscrimination are not by themselves guarantors of net neutrality norms. Canada's Telecommunications Act, e.g., may prevent overtly discriminatory practices, but in practice Canada may have legitimized needlessly conservative and possibly anti-competitive incumbent practices.

It is clear that DPI use tends to provoke regulatory processes and its use is then affected by the outcome of regulatory processes. The impact (or lack thereof) of such regulatory processes seems to be detectable in the Glasnost results. In this comparison, opposition by an organized movement and the threat of regulation by a regulator with no authority was actually more effective at enforcing net neutrality norms than a regulatory authority with a law fully embodying common carrier and nondiscrimination norms.

References

Aghasaryan, A., M. Kodialam, et al. (2010). "Personalized Application Enablement by Web Session Analysis and Multisource User Profiling." Bell Labs Technical Journal **15**(1): 67-76.

Allot, C. (2007). Network Visibility and Service Management Utilizing Deep Packet Inspection (DPI) Technology, Allot Communications. **White Paper:** http://www.allot.com/index.php?option=com_docman&task=cat_view&Itemid=96&gid=88888893.

Beer, J. D. and C. D. Clemmer (2009). "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?" Jurimetrics **49**: 375-409.

Bendrath, R. and M. Mueller (2011). "The End of the Net as we Know it? Deep Packet Inspection and Internet Governance." New Media and Society.

Collins, R. (2010). "The Privacy Implications of Deep Packet Inspection Technology: Why the next wave in online advertising shouldn't rock the self-regulatory boat." Georgia Law review **44**(2): 545-577.

Coward, M. (2009). "Deep packet inspection optimizes mobile applications." EDN **54**(19): 37-40.

Dischinger, M., M. Marcon, et al. (2010). Glasnost: Enabling End Users to Detect Traffic Differentiation. Proceedings of 7th USENIX Symposium on Networked Systems Design and Implementation (NSDI).

Finnie, G. (2009). ISP Traffic Management Technologies: The State of the Art. Report prepared for The Canadian Radio Television and Telecommunications Commission. Ottawa, Canadian Radio Television and Telecommunications Commission, http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm.

Frieden, R. M. (2007) "Internet Packet Sniffing and Its Impact on the Balance of Power " http://works.bepress.com/robert_frieden/2/.

Kim, S. and J. Y. Lee (2007). "A system architecture for high-speed deep packet inspection in signature-based network intrusion prevention." Journal of Systems Architecture **53**(5-6): 310-320.

McTaggart, C. (2008). Net Neutrality and Canada's Telecommunications Act. Fourteenth Biennial National Conference on New Developments in Communications Law and Policy, Law Society of Upper Canada. Ottawa, SSRN http://ssrn.com/abstract=1127203.

Meyer, T. and L. V. Audenhove (2010). "Graduated response and the emergence of a European surveillance society." Info **12**: 69-79.

Mochalski, K. and H. Schulze (2009) "Deep packet inspection, net neutrality, Internet bandwidth management." 12.

Proch, D. and R. Truesdell (2009). Plumb the depths of deep packet inspection. Electronic Design. **57**: 47-50.

Rossenhövel, C. (2008) "Peer-to-Peer Filters: Ready for Internet Prime Time?" Internet Evolution.

Vorhaus, D. and M. Bieberich (2007). Knowledge Is Power: The Role of Deep Packet Inspection in Generating New Revenue Streams. Boston, Yankee Group: http://www.allot.com/index.php?option=com_docman&task=cat_view&Itemid=96&gid=88888893.

Yoo, C. (2006). "Network Neutrality and the Economics of Congestion." Georgetown Law Journal **94**(Journal Article): 1847.