Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

Philippa Lawson
Director
(613) 562-5800 x2556
plawson@uottawa.ca

25 July 2008

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

Dear Commissioner Stoddart:

Re: Rogers Communications Inc.'s Use of Deep Packet Inspection for Traffic-Management Purposes: PIPEDA Complaint

1. This is a complaint under s.11 of Part I of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), regarding the unnecessary and non-consensual collection and use of personal information by Rogers Communications Inc. ("Rogers") through the use of "Deep Packet Inspection" ("DPI") technology. Our attention has been drawn to this matter by individual internet users and media reports. This complaint follows a similar complaint that we recently filed against Bell Canada.

2. In brief, we understand that Rogers is engaging in internet "traffic management" practices that involve the inspection of internet traffic headers and content, both of which contain information that can be linked to internet subscribers. Rogers purports to classify traffic for the purposes of network optimization. Despite these claims by Rogers, it is not clear that such practices – i.e., those involving the collection and use of personal information – are *necessary* to ensure network integrity and quality of service. Moreover, it is not clear that Rogers's subscribers whose traffic is being inspected have consented to the inspection and use of their personal data for this purpose. Further, Rogers does not make readily available to individuals specific information about these practices.

3. Based on our research, we also suspect that Rogers (and other Canadian ISPs) may be engaging or preparing to engage in the collection of subscriber data via DPI in order to target advertising at individual users. Again, we question whether such collection and use of personal data is necessary for advertising purposes, and whether subscribers have

consented to such uses of their personal data. Please see our separate letter requesting that you initiate an industry-wide investigation into this issue.

4. We therefore submit that Rogers is violating Principles 4.3, 4.4, and 4.8 of *PIPEDA*, Schedule 1 insofar as it is failing to:

   a. Obtain informed consent from affected individuals to the collection and use of their personal information gleaned from traffic data for purposes of traffic management and/or targeted marketing; (Principle 4.3);

   b. Limit the collection of personal information to that which is necessary for its stated purposes (Principle 4.4); and

   c. Make readily available to the public specific information about its policies and practices insofar as they involve the collection and analysis of personal information for traffic management and/or targeted marketing purposes (Principle 4.8).

I FACTS

A. About Rogers

5. Rogers is Canada's largest cable television service provider. It also offers high-speed Internet access and telephone services to both residential and business customers.[1] Through its subsidiary Rogers Cable Inc., Rogers sells internet service to approximately 1.5 million residential subscribers and has established 35,000 broadband data circuits for businesses.[2] These retail internet services are not regulated by the CRTC.

6. Rogers is required by the CRTC to sell wholesale higher speed internet access to other ISPs that in turn sell residential and business internet services to their own subscribers.[3] This wholesale service is regulated by the CRTC and is governed by a tariff.[4]

B. Internet Traffic Management and Deep Packet Inspection

7. Cable and telecommunications companies engage in internet traffic shaping on the grounds that the practice is required to most efficiently manage their scarce network

[1] See Rogers.com, "Investor Relations", online: <http://your.rogers.com/investorrelations/investor_overview.asp> and see Rogers.com, "Investor Relations: Rogers Cable", online: <http://your.rogers.com/investorrelations/rogers_cable.asp>.
[2] *Ibid*.
[3] CRTC Order 2000-789, *Terms and rates approved for large cable carriers' higher speed access to service*, online: CRTC <http://www.crtc.gc.ca/archive/eng/Orders/2000/O2000-789.htm> at paras.12 and 24.
[4] CRTC Order 2001-92, *Terms and rates approved for large cable carriers' higher speed access to service – Follow up to Order 2000-789*, online: CRTC <http://www.crtc.gc.ca/archive/eng/Orders/2001/O2001-92.htm> at para.1.

capacity. Traffic shaping critics have questioned this rationale, noting that other motives behind ISP traffic shaping might include slowing down competitor traffic (either a competing ISP purchasing wholesale network access or a user sharing content via P2P that competes with the content provided by ISPs and their affiliates). These critiques are underscored by the way that DPI has been marketed. Vendors of DPI technology promote their services to ISPs as leveraging network management and ownership for increased profit.[5]

8. Internet traffic shaping practices have typically focused on identifying and slowing down Peer-to-Peer ("P2P") traffic during peak hours of usage for the alleged purpose of ensuring adequate bandwidth availability for other users. In order to distinguish P2P traffic from other types of traffic, ISPs typically use DPI technologies. Across a network, information is grouped into packets containing both a header and contents. Our research suggests that DPI differs from basic network management in that it examines the contents (commonly called the "payload") rather than just the header of the data packet.

9. According to one authority, Deep Packet Inspection:

> … is a computer networking term that refers to devices and technologies that inspect and take action based on the contents of the packet (commonly called the "payload") rather than just the packet header. The following analogy helps clarify the role of DPI:
>
> > A packet is analogous to a physical postal mail message. The address on the outside of the envelope is analogous to the "packet header" and the information inside the envelope is analogous to the "payload." DPI is analogous to taking action on that mail message not only based on the address on the envelope, but also making considerations based on the contents of the envelope.
>
> The analogy serves as a fair functional description, but falls short of describing the need for DPI. While privacy is a legitimate [sic], the use and importance of DPI will continue to grow and examples of its value are provided in the next paragraph. A more general term called "Deep Packet Processing" (DPP) that encompasses actions taken on the packet such as modification, blocking/filtering, or redirection is also gaining use. Today, DPI and DPP are often used interchangeably.[6]

10. Another source states:

---

[5] Letter from CAIP to CRTC (3 April 2008), *Re: Part VII Application by the Canadian Association of Internet Providers Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" its Wholesale ADSL Access Services*, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/895702.pdf> [CAIP letter]; for an example of vendor promotional literature, see the discussion of the need for network owners to leverage their position. Cisco Systems, "Cisco Service Control Engine (SCE) Software Configuration Guide, Rel. 3.1 – General Overview [Cisco Service Control Operating System Software]", online: <http://www.cisco.com/en/US/products/ps6134/products_configuration_guide_chapter09186a0080849902.html> [Cisco General Overview].

[6] [d]packet.org, "Introduction to Deep Packet Inspection/Processing," online: <https://www.dpacket.org/introduction-deep-packet-inspection-processing>.

> The "deep" in deep packet inspection refers to the fact that these boxes don't simply look at the header information as packets pass through them. Rather, they move beyond the IP and TCP header information to look at the payload of the packet. The goal is to identify the applications being used on the network, but some of these devices can go much further; those from a company like Narus, for instance, can look inside all traffic from a specific IP address, pick out the HTTP traffic, then drill even further down to capture only traffic headed to and from Gmail, and can even reassemble e-mails as they are typed out by the user.
>
> But this sort of thing goes beyond the general uses of DPI, which is much more commonly used for monitoring and traffic shaping. Before an ISP can shape traffic, it must know what's passing through its system. Without DPI, that simple-sounding job can be all but impossible. "Shallow" packet inspection might provide information on the origination and destination IP addresses of a particular packet, and it can see what port the packet is directed towards, but this is of limited use."
>
> …..
>
> Looking this closely into packets can raise privacy concerns: can DPI equipment peek inside all of these packets and assemble them into a legible record of your e-mails, web browsing, VoIP calls, and passwords? Well, yes, it can. In fact, that's exactly what companies like Narus use the technology to do, and they make a living out of selling such gear to the Saudi Arabian government, among many others.
>
> Texas disaster recovery and managed services company Data Foundry objects to network operators doing this deep level of inspection. In a recent FCC filing, the company charged that "broadband providers' AUP/TOS/Privacy Policies, in combination with Deep Packet Inspection, allow intrusive monitoring of the content and information customers transmit or receive. This contractual and technical capability interferes with and may well eliminate all sorts of privileges presently recognized under law... Broadband service providers have no justifiable reason to capture this information.[7]

11. Cisco Systems states that its traffic management "SCE platform is designed to support classification, analysis, and control of Internet/IP traffic." The platform presents network owners with the ability to perform "[a]pplication-level drilling into IP traffic for real-time understanding and controlling of usage and content at the granularity of a specific subscriber." [8] Further, Cisco offers

> The ability to map between IP flows and a specific subscriber in order to maintain the state of each subscriber transmitting traffic through the SCE platform and to enforce the appropriate policy on this subscriber's traffic.[9]

12. Cisco further adds that

> "Service Control **enables service providers to create profitable new revenue streams while capitalizing on their existing infrastructure**. With the power of Service Control, service providers have the ability to analyze, charge for, and control IP network traffic at multigigabit wire line speeds. The Cisco Service Control solution also gives service providers the tools they need to identify and target high-margin content-based services and to enable their delivery. …[C]apturing real profits from IP services requires more than simply running those services over data links; it requires **detailed monitoring and precise, real-time control and**

[7] Nate Anderson, "Throttle me this: An introduction to DPI" (July 2007), online: <http://arstechnica.com/articles/culture/deep-packet-inspection-meets-net-neutrality.ars>
[8] Cisco General Overview, *supra* note 5.
[9] *Ibid*.

> **awareness of services as they are delivered**. Cisco provides Service Control solutions that allow the service provider to bridge this gap."[10]

C. Rogers's Traffic Management Practices

13. Rogers has acknowledged that it is engaging in Internet traffic management at the retail level. Rogers argues its Internet traffic management is necessary to maintain the network's ability to meet basic usage demands.[11]

14. It is not clear whether, when or how Rogers advised its retail subscribers of the fact that it was and is applying traffic management and shaping techniques. However, Rogers has been the subject of many user complaints about its DPI and traffic shaping practices.[12]

15. Media and user reports have alleged that Rogers uses the Cisco pCube Service Control system to engage in DPI.[13] In response to user complaints about the insertion of Rogers messaging into unrelated web sites, Rogers's spokespeople acknowledged that the company is testing out different technologies and one spokesperson confirmed that it is employing DPI technologies.[14]

16. In late April 2008, Nadir Mohammed, Rogers President and Chief Operating Officer of the Communications division (which includes Rogers Cable), assured *The Toronto Star* that Rogers would continue to throttle internet traffic, despite introducing a new fee for heavy bandwidth users.[15] In addition, Prof. Michael Geist, the Canada Research Chair of Internet and E-commerce Law, wrote on his blog in March 2008 that Rogers

---

[10] *Ibid*. [Bold added].
[11] Peter Nowak, "Rogers says its internet interference is necessary, but minimal" *CBC News* (June 10, 2008), online: <http://www.cbc.ca/technology/story/2008/06/10/tech-rogers.html> [Rogers's defence]; Michael Geist, "ISP must come clean on 'traffic shaping'" *The Toronto Star* (April 16. 2007), online: <http://www.thestar.com/article/203408>; See further Matt Hartley, "CRTC orders Bell to prove Net 'shaping' needed" *The Globe and Mail* (May 16, 2008), online: <http://www.theglobeandmail.com/servlet/story/RTGAM.20080516.wrthrottle16/BNStory/Technology/home%3Cbr%3E>.
[12] See www.azureuswiki.com, "Bad ISPs", online: <http://www.azureuswiki.com/index.php/Bad_ISPs#Canada; and Julie Fortier, "Caught in the Throttle", *The Ottawa Business Journal* (September 4, 2007), <http://www.ottawabusinessjournal.com/319629855570564.php>.
[13] "Rogers HiSpeed FAQ: 2 Policies" *DSL Reports*, online: dslreports.com, <http://www.dslreports.com/faq/rogers/2_Rogers_Policies>.
[14] Sarah Lai Stirland, "In Test Canadian ISP splices itself into Google Homepage" *Wired: Threat Level Blog* (December 10, 2007), online: < http://blog.wired.com/27bstroke6/2007/12/canadian-isps-p.html>; and Digital Home Canada, "Rogers Tampers with Digital Home web pages" (April 9, 2008), online: <http://www.digitalhome.ca/content/view/2436/206/1/1/>.
[15] Chris Sorensen, "Rogers to limit 'free' Internet", *The Toronto Star* (April 30, 2008), online: <http://www.thestar.com/Business/article/419741>.

representatives confirmed that throttling would not stop with the implementation of the new usage fees.[16]

17. Rogers, however, has not been consistently forthcoming about what exact practices it is engaging in and why. In October 2007, Prof. Geist wrote, "[Rogers's] website does not include a single mention of traffic shaping or limits on peer-to-peer applications and company spokespersons have provided inconsistent explanations for what is happening behind the scenes."[17] In March 2008, five months later, Prof. Geist noted that despite confirming that it does engage in throttling, Rogers had still not addressed its lack of disclosure to subscribers and the company would only say that it was working to resolve the issue.[18] In June 2008, Dermot O'Carroll, Rogers's Senior Vice-President of engineering and network operations, held a briefing with reporters and defended throttling as necessary for network management.[19] Still, Rogers has not disclosed specifically how they are shaping web traffic.

18. In the United States, Comcast, a large ISP, is the subject of at least one lawsuit and an investigation by the Federal Communications Commission ("FCC") for its traffic management practices that, like Rogers's practices, involve the inspection and differential treatment of internet traffic. On July 11 FCC Chairman Kevin Martin announced that he was recommending enforcement action against Comcast for its throttling practices and that the order would be voted on by the other commissioners at an open meeting on August 1.[20]

19. Comcast had initially claimed that its method of traffic management was necessary in order to reduce network congestion on its network. The Chairman of the FCC refuted Comcast's network congestion claims, noting that:

> It does not appear that this technique was used only to occasionally delay traffic at particular nodes suffering from network congestion at that time. Indeed, based on the testimony we have received thus far, this equipment was typically deployed over a wider geographic area or system and it is not even capable of knowing when an individual cable segment of the network is congested. This equipment blocks uploads of a significant portion

[16] Michael Geist, "Rogers Broadband: New Caps but No Transparency", *Michael Geist* (March 17, 2008), online: <http://www.michaelgeist.ca/content/view/2760/125/> [New Caps but No Transparency].
[17] Michael Geist, "Canadians deserve better ISP transparency", *The Toronto Star*, (October 8, 2007), <http://www.thestar.com/article/264504>.
[18] Geist, New Caps but No Transparency, *supra* note 16.
[19] Nowak, Rogers's defence, *supra* note 11.
[20] Reuters, "FCC seeks to punish Comcast in Internet probe: report", *Reuters.com*, (July 11, 2008), online: <http://www.reuters.com/article/internetNews/idUSBNG1334420080711>.

> of subscribers in that part of the network regardless of the actual levels of congestion at that particular time.[21]

20. Comcast subsequently acknowledged that its use of traffic shaping programs involving the identification and slowing down of specific types of traffic (namely, P2P) was not in fact necessary in order to maintain the integrity of its network, and announced that it would migrate by the end of 2008 to a bandwidth-management technique that is "protocol agnostic".[22] Trials of three alternative techniques are set to take place this summer.[23]

II APPLICATION OF PIPEDA TO ROGERS'S TRAFFIC MANAGEMENT PRACTICES

A. Rogers is collecting and using "personal information" via Deep Packet Inspection technology for traffic management purposes

21. Section 2 of *PIPEDA* defines "personal information" as "… information about an identifiable individual …." Any factual information therefore constitutes personal information as long as it can be linked to an identifiable individual.[24] Information about data packets gathered by ISPs through the use of DPI for traffic shaping is (or can be) associated with identifiable subscribers via the IP addresses attached to those data packets. Moreover, as noted above, the data typically examined by DPI systems involve much more than IP addresses: the whole purpose of DPI is to "open the envelope" in order to discern details about the traffic such as its type or source.

22. The evidence is clear that DPI technologies permit the collection and use of personal data about internet subscribers. The extent to which Rogers is actually taking advantage of this capability is less clear. However, the literature on DPI suggests that DPI necessarily

---

[21] United States Senate Committee on Commerce, Science and Transportation, *Opening Remarks (as delivered) by Kevin J. Martin, FCC, Chairman*, 22 April 2008 (archived webcast) <http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=4c66f979-3001-490a-a985-5be63951adb7>.

[22] Todd Spangler, "Comcast Pledges to Help Bittorrent, not Hinder it", *Multichannel News*, (March 27, 2008), <http://www.multichannel.com/article/CA6545414.html>.

[23] Peter Svensson, "Comcast to test new way to manage Internet traffic jams", *SiliconValley.com* (June 3, 2008), online: <http://www.siliconvalley.com/news/ci_9467453>.

[24] Office of the Privacy Commissioner of Canada, *A Guide for Businesses and Organizations: Your Privacy Responsibilities* (updated March 2004) "Definitions: Personal information," online: <http://www.privcom.gc.ca/informaiton/guide_e.asp> [Guide]; PIPEDA Case Summary #319, "ISP's anti-spam measures questioned" (8 November 2005), online: <http://www.privcom.gc.ca/cf-dc/2005-319_20051103_3.asp>.

involves some collection and/or use of personal data in order for it to be a useful traffic shaping or behavioural targeting tool for ISPs.

23. Even if Rogers is somehow able to limit the data it inspects via DPI to non-personal data, we remain concerned about the longer term viability of any such limitation, and the pressure on Rogers (and other ISPs) to use DPI to distinguish among traffic in ways that necessarily involve the collection and use of personal data.

B. Principle 4.3: Knowledge and Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

24. Rogers has not obtained informed consent to traffic shaping or behavioural targeting. Neither the Rogers's *Privacy Policy* (which applies company-wide, not just to internet service) nor any of the other privacy documents or statements to which Rogers directs its customers actually refer to Rogers's use of deep packet inspection technology for traffic shaping or behavioural targeting.

25. Rogers's only mention of possible user surveillance is in the company's *Acceptable Use Policy* for internet subscribers which states that "we may monitor or investigate content or your use of our networks, including bandwidth consumption."[25]

26. However, the Rogers *Privacy Policy* sets out five broad purposes for which the company collects, uses and discloses personal information, none of which directly refers to DPI, the linking of data packets to identifiable subscribers, or behavioural targeting:

- To provide a positive customer experience, and deliver, bill for, and collect payment for products and services;
- To understand customer requirements and make information available regarding products and services offered by Rogers and its agents, dealers and related companies;
- To manage and develop Rogers business and operations;
- To meet legal and regulatory requirements; and
- To obtain credit information or provide it to others. [26]

27. A link on the *Privacy Policy* page directs visitors who want more information regarding privacy to the Rogers *FAQ Privacy Category*.[27] Frequently asked question 7 ("**How do**

[25] *Acceptable Use Policy Rogers Yahoo! Hi-Speed Internet Services*, online: Rogers Yahoo! Hi-Speed Internet <http://www.rogershelp.com/yahoo/downloads/agreements/AUP.PDF>.
[26] *Privacy Policy*, online: Rogers.com <http://your.rogers.com/privacy1.asp>.

the Rogers Group of Companies use information gathered about me?") sets out the purposes for which the collected information will be used. The FAQ does not refer to the linking of identifiable subscribers with specific data packets or collecting data to facilitate directing targeted advertising from unrelated companies toward the individual.

28. To summarize, neither Rogers's *End User Agreement*, its *Acceptable Uses Policy*, its *Privacy Policy*, nor its FAQ disclose Rogers's alleged practice of inspecting data packets that are or can be linked to identifiable individuals, for traffic shaping, behavioural targeting or other purposes.

29. Consent is only meaningful when affected individuals understand that to which they are consenting. If Rogers is relying on its published policies as set out above to inform its customers and obtain their implied consent to its use of DPI for traffic management purposes, we submit that it has not met the standard of informed consent required by Principle 4.3 of Schedule 1 to *PIPEDA*.

C. Principle 4.4: Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.

30. Even if Rogers were to have obtained informed consent from its subscribers to its traffic shaping use of DPI, the evidence suggests that Rogers can manage its network adequately without inspecting the content of user communications.

31. First, after pressure from the FCC and the U.S. public, Comcast has announced that it will change its traffic management practices so as not to discriminate among different applications. While it is not clear to what extent Comcast's new approach to traffic management will involve the inspection of personal information, the company has said that it will "migrate to techniques that the Internet community will find to be more transparent".[28]

---

[27] Rogers, FAQ Privacy Category, online: Rogers.com <http://shoprogersfaq.custhelp.com/cgi-bin/shoprogersfaq.cfg/php/enduser/std_alp.php?p_sid=2NAKmcIh&p_lva=&p_li=&p_page=1&p_prod_lvl1=204&p_prod_lvl2=205&p_search_text=&p_new_search=1&p_search_type=4&p_sort_by=dflt >.

[28] Todd Spangler, "Comcast Pledges to Help Bittorrent, not Hinder it", *Multichannel News*, (March 27, 2008), <http://www.multichannel.com/article/CA6545414.html>. See above text at note 22.

32. Second, Rogers has not provided empirical or verifiable evidence that the quality of its Internet network has been impaired by congestion, or that its traffic management techniques actually alleviate network congestion.

33. Third, there are other, less privacy invasive, means for Rogers to address any network congestion problems that it is experiencing. It can, for example, invest in more infrastructure to accommodate the additional demand generated by P2P traffic. Alternatively, it is our understanding Rogers could:

a. set limits on the amount of data per second that any user can transmit on the network
b. set dynamic data limits that relax when congestion is low and increase when congestion is high
c. cache popular files (in a non-discriminatory fashion)
d. work with protocol/application developers to develop application and network level congestion mechanisms
e. institute per-user bandwidth caps and/or metered pricing (which it is now doing), and/or
f. develop business models to encourage heavy bandwidth usage during off-peak hours.

34. Because it is not necessary for the purpose of reasonable network management, Rogers's use of DPI for traffic shaping violates Principle 4.4 of Schedule 1 to *PIPEDA.*

D. Principle 4.8: Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

35. As noted above, neither Rogers's *Privacy Policy*, *End-User Agreement*, nor its *Acceptable Use Policy* state that Rogers will collect Rogers Yahoo! Hi-Speed subscribers' personal information in examining the nature of the data packets they send or receive, or that it will use the information garnered from this examination to limit their ability to use the Internet at certain periods. In particular, Rogers's *Privacy Policy* does not provide any specific references to or information about its use of DPI for traffic shaping.

36. Rogers is failing to comply with Principle 4.8 by not disclosing in a clear and conspicuous manner to the public its use of DPI for traffic management.

III REQUEST FOR INVESTIGATION AND FINDING

37. On the basis of the above allegations, we request that you investigate Rogers's use of DPI for traffic management purposes with a view to its compliance with *PIPEDA*. As noted above, we are also requesting by way of a separate letter that you investigate the actual and potential use by Rogers and other Canadian ISPs of DPI for behavioural targeted advertising purposes.

38. Moreover, as noted above, there is evidence that a number of other Canadian ISPs are engaging in similar practices for similar purposes. We urge you to investigate the use of DPI by other Canadian ISPs, and to issue guidelines to the industry at large.

39. We await your findings, and response. Should you have any questions, please do not hesitate to contact the undersigned.

Sincerely,

Original Signed
Rishi Hargovan
Summer Intern

Original Signed
Philippa Lawson
Director

cc: Bell Canada, Rogers Communications Inc., Shaw Communications Inc., Eastlink, CAIP