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: EastLink'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 EastLink ("EastLink") 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. We believe that you should investigate the privacy implications of current and intended uses of DPI by all large ISPs in Canada.

2. In brief, we understand that EastLink 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. EastLink purports to classify traffic for the purposes of network optimization. Despite these claims by EastLink, 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 EastLink's subscribers whose traffic is being inspected have consented to the inspection and use of their personal data for this purpose. Further, EastLink does not make readily available to individuals specific information about these practices.

3. Based on our research, we also suspect that EastLink (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 EastLink 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 EastLink

5. Based in Halifax, EastLink is Canada's fifth largest cable television service provider. It offers high-speed Internet access and telephony services.[1] Through its cable network, EastLink provides high-speed internet service across Atlantic Canada.[2] These retail internet services are not regulated by the CRTC. In 2002, EastLink Cable Systems started a commercial relationship with Ellacoya Networks, a company that provides network management technology and services.[3]

B. Internet Traffic Management and Deep Packet Inspection

6. Cable and telecommunications companies engage in internet traffic shaping on the grounds that the practice is required to most efficiently manage their scarce network capacity. Traffic shaping critics have questioned this rationale, noting that other motives behind ISP traffic shaping might include slowing down competitor traffic (either a

[1] EastLink, "About EastLink", online: <http://www.eastlink.ca/about/>.
[2] *Ibid*.
[3] Marguerite Reardon, "Is Ellacoya on the Comeback Trail?", *Light Reading* (January 13, 2003), online: <http://www.lightreading.com/document.asp?doc_id=26784>.

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.[4]

7. 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.

8. 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.[5]

9. Another source states:

> 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

[4] 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].

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

> 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.[6]

10. In 2005, Ellacoya stated that it provides "intelligent bandwidth management solutions" and "enables application traffic that has specific bandwidth … requirements to be prioritized on a per-subscriber basis, ensuring the application's proper performance regardless of the overall traffic load on the network."[7] More specifically, Ellacoya's IP Service Control System

> … **identifies subscribers, classifies and controls applications on a per-subscriber basis**, improves performance and customer satisfaction, and delivers revenue-generating IP services. It is the only company that provides the granular network visibility and tools necessary to enable more compelling applications and competitive service offerings.[8]

11. Approaches to DPI are evolving. Just over a year ago, for example, Ellacoya announced that it was launching a new "evolution of deep packet inspection (DPI) technology for service providers that it would make available beginning in March 2007. According to Ellacoya, it can now track individual subscribers' online activities:

---

[6] Nate Anderson, "Throttle me this: An introduction to DPI" (July 2007), online: <http://arstechnica.com/articles/culture/deep-packet-inspection-meets-net-neutrality.ars>

[7] Ellacoya Networks, "Ellacoya Networks Attracts New Investors in $13.5M Financing" News Release (Merrimack, New Hampshire: 18 July 2005), online: <http://www.ellacoya.com/news/pdf/2005/Ellacoya2005Funding.pdf >.

[8] *Ibid*. (bold font added).

> The Ellacoya e100 is a carrier-class and carrier-scale network platform that enables providers to identify and manage each packet of network traffic dynamically by subscriber, service type, time-of-day, and more. Together with Ellacoya's rich suite of software applications, the e100 can: provide granular reports on network usage; manage traffic dynamically with precision; ensure VoIP quality; identity [*sic*] and prevent network threats; and provide the basis for quota management, differentiated service plans and quality-assured premium services (IPTV, VoIP, streaming video).
>
> …
>
> **Deeper into the Packet – Precision Service Marketing and Management**
>
> The Ellacoya solution identifies applications through signatures in the data packet and through sophisticated traffic-pattern analysis to provide unprecedented visibility into subscriber usage, subscriber-specific service activity and service quality on a per-application basis. Uniquely, as new applications are discovered on the network, customers can download software signatures in real-time to the Ellacoya platform to ensure new applications can be identified as soon as possible. The e100 adds more granular application detection to identify applications within applications; for example streaming video, voice-over-IP and gaming can be detected within a Web (HTTP) download. As a result, the platform delivers comprehensive granular reports on subscriber and application usage to enable effective service marketing based on real subscriber behavior data. "Being able to track customer service usage from the application layer is an excellent way to optimize marketing programs and service creation initiatives based on actual traffic patterns" said Matt Davis, director of consumer multiplay services at analyst firm IDC. "Ellacoya is one of the pioneers in this area, and this kind of technology can provide an invaluable tool for marketing executives."[9]

C. EastLink's Traffic Management Practices

12. Though EastLink has not explicitly acknowledged that it is engaging in Internet traffic management at the retail level, there have been consumer complaints and media reports alleging the it does.[10] It is not clear whether, when or how EastLink advised its retail subscribers whether or not it was and is applying traffic management and shaping techniques.

13. A 2007 media report cited an anonymous network manager who admitted that EastLink prioritizes one form of traffic over another. The account was confirmed by Steve Irvine, EastLink's Director of Internet Engineering and Operations and by an EastLink customer service representative named Adam.[11]

---

[9] Ellacoya Networks, "Ellacoya Brings Unmatched Scale and intelligence to Broadband Service Optimization" News Release (25 January 2007) online: Ellacoya Networks online: <http://www.ellacoya.com/news/pdf/2007/Ellacoya_e100PressRelease.pdf> (bold font in original; underlining added).

[10] See www.azureuswiki.com, "Bad ISPs", online: <http://www.azureuswiki.com/index.php/Bad_ISPs#Canada; Vincenzo Ravina, "Bandwidth Battles", *The Coast* (September 20, 2007), online: <http://thecoast.ca/119846.113118body.lasso?-token.folder=2007-09-20&-token.story=150881.113118&-token.subpub=>.

[11] *Ibid*.

14. 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 EastLink'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.[12]

15. 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 of subscribers in that part of the network regardless of the actual levels of congestion at that particular time.[13]

16. 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".[14] Trials of three alternative techniques are set to take place this summer.[15]

II APPLICATION OF PIPEDA TO EASTLINK'S TRAFFIC MANAGEMENT PRACTICES

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

---

[12] Reuters, "FCC seeks to punish Comcast in Internet probe: report", *Reuters.com*, (July 11, 2008), online: <http://www.reuters.com/article/internetNews/idUSBNG1334420080711>.

[13] 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>.

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

[15] 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>.

17. 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.[16] 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.

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

19. If EastLink 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 EastLink (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.

20. EastLink has not obtained informed consent to this practice. Neither the EastLink *Privacy Policy*[17] (which applies company-wide, not just to internet service), the EastLink *Code of Fair Information Practices*,[18] nor any other privacy document or statement to which EastLink directs its customers explicitly discloses EastLink's use of deep packet inspection technology for traffic shaping or behavioural targeting.

---

[16] 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>.

[17] *Customer Privacy Policy*, online: EastLink.ca <http://www.eastlink.ca/about/legal/documents/EastLink_Customer_Privacy_Policy-May2006.pdf> ["Customer Privacy Policy"].

[18] *Code of Fair Information Practices*, online: EastLink.ca <http://www.eastlink.ca/about/legal/documents/EastLink_Code_of_Fair_Information_Practices-May2006.pdf>.

21. EastLink mentions the possibility of traffic shaping in the *EastLink Internet Acceptable Use Policy*. The document states that "EastLink reserves the right to set specific limits for Bandwidth Usage and other elements of service at any time."[19] It adds "EastLink reserves the right to monitor bandwidth, usage, and content from time to time to operate the Services; to identify violations of this Policy; and/or to protect the network and EastLink users."[20]

22. In addition, EastLink reserves the right to take remedial action:

> "EastLink may take any responsive actions it deems appropriate. Such actions include, but are not limited to, temporary or permanent removal of content, cancellation of newsgroup posts, filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Services. ... The above-described actions are not EastLink's exclusive remedies and EastLink may take any other legal or technical action it deems appropriate."

23. The EastLink *Privacy Policy* sets out three purposes for which the company collects, uses and discloses personal information, none of which directly refers to DPI or the linking of data packets to identifiable subscribers:

> (a) provide better customer service (e.g., by keeping customers informed of new products, services and promotions);
> (b) help us better understand your communications needs and preferences so that we can develop, enhance, market and provide products and services (e.g., we may analyze your use of our products and services to help us provide better product recommendations and special offers that we think will interest you); and
> (c) manage and develop our business operations.[21]

24. To summarize, neither EastLink's *Terms of Service*, its *Internet Acceptable Use Policy*, *Code of Fair Information Practice*, nor its *Privacy Policy* discloses EastLink's alleged practice of inspecting data packets that are or can be linked to identifiable individuals, for traffic shaping, behavioural targeting or other purposes.

25. Consent is only meaningful when affected individuals understand that to which they are consenting. If EastLink 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

[19] *EastLink Internet Acceptable Use Policy*, online: EastLink.ca <http://www.eastlink.ca/about/legal/aup.asp>.
[20] *Ibid.*
[21] Customer Privacy Policy, *supra* note 17.

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

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

27. 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".[22]

28. Second, EastLink 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.

29. Third, there are other, less privacy invasive, means for EastLink 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 EastLink 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.

[22] Todd Spangler, "Comcast Pledges to Help Bittorrent, not Hinder it", *Multichannel News*, (March 27, 2008), <http://www.multichannel.com/article/CA6545414.html>. See text above at note 14.

30. Because it is not necessary for the purpose of reasonable network management, EastLink'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.

31. As noted above, neither EastLink's *Terms of Service*, its *Internet Acceptable Use Policy, Code of Fair Information Practice*, nor its *Privacy Policy* discloses that EastLink will collect 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, EastLink's *Privacy Policy* does not provide any specific references to or information about its use of DPI for traffic shaping.

32. EastLink 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

33. On the basis of the above allegations, we request that you investigate EastLink's use of DPI for traffic management 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.

34. 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.

35. 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