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

9 May 2008

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

Dear Commissioner Stoddart:

Re: Bell Canada/Bell Sympatico Use of Deep Packet Inspection: 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 Bell Canada and Bell Sympatico (collectively, "Bell") through the use of "Deep Packet Inspection" ("DPI") technology. Our attention has been drawn to this matter by individual internet users, media reports, and most recently, an application filed with the Canadian Radio-television Telecommunications Commission (CRTC) on 3 April 2008 by the Canadian Association of Internet Providers (CAIP).[1]

2. In brief, we understand that Bell 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, purportedly to classify traffic for purposes of network optimization. Such practices – i.e., those involving the collection and use of personal information - are not *necessary* to ensure network integrity and quality of service. Moreover, subscribers whose traffic is being inspected have not consented to the inspection and use of their data for this purpose. Finally, Bell does not make readily available to individuals specific information about these practices.

---

[1] 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].

3. We submit that Bell is violating Principles 4.3, 4.4, and 4.8 of *PIPEDA*, Schedule 1 by failing to:

   a. Obtain informed consent from affected individuals to the collection and use of their personal information for the purpose of traffic management (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 traffic management policies and practices insofar as they involve the collection and analysis of personal information (Principle 4.8).

I FACTS

A About Bell

4. Bell is Canada's largest telephone and telecommunications company and is owned and controlled by Bell Canada Enterprises. Bell sells Internet service directly to more than 2 million business and residential subscribers through its Sympatico division.[2] These retail internet services are not currently regulated by the CRTC.

5. Bell also sells wholesale Internet access to other ISPs that in turn sell residential and business internet services to their own subscribers, of whom there are approximately 100,000. These wholesale services are regulated by the CRTC by way of tariffs. We understand that virtually all independent ISPs operating in Bell Canada's traditional service territory use Bell's tariffed Internet services.

6. In addition, Bell Enterprise offers network management tools and services to other businesses.[3] In this respect, we note that in 2005, the venture-investment arm of BCE invested in a company that designs network traffic management tools using Deep Packet Inspection technology – Ellacoya Networks (Ellacoya).[4]

B. Internet Traffic Management and Deep Packet Inspection

7. ISPs engage in traffic shaping in order purportedly to make the most efficient use of their networks. Critics have suggested, however, that there may be other motives behind traffic shaping by ISPs, including slowing down of competitor traffic (whether the

---

[2] Bell, *Supplementary Financial Information: Fourth Quarter 2007* at 7 ("High Speed Internet subscribers EOP") online: BCE <http://www.bce.ca/data/documents/reports/en/2007/q4/2007q4-si-en.pdf>.

[3] See www.bell.ca/enterprise

[4] Acquired by Arbor Networks on 12 February 2008 (http://www.ellacoya.com).

competitor is a wholesale ISP or a user sharing competing content via P2P), and development of methods by which to extract more revenues from internet traffic.[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 Deep Packet Inspection technologies. DPI 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:

> "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-

[5] CAIP Letter, *supra* Note 1.

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

> 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. 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."[8] More specifically, Ellacoya's IP Service Control System

> … i**dentifies 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. [9]

12. 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:

> 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

---

[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] 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 >.

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

> 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."[10]

C. Bell's Traffic Management Practices

13. Bell is engaging in Internet traffic management at both the retail and wholesale levels. Bell describes its Internet traffic management technique "as a mechanism to allow for a better allocation of bandwidth for all users that share a common network",[11] and has said that it applies the technique to "uploads and downloads of P2P traffic during peak periods."[12]

14. On 28 March 2008 Bell wrote to some of its wholesale ISP customers and confirmed that it had begun to apply traffic management and shaping techniques to its own Internet subscribers and to the subscribers of CAIP members.[13] It is not clear whether, when or how the Company advised its retail Sympatico subscribers of the fact that it was and is applying traffic management and shaping techniques.

15. Other ISPs in Canada and elsewhere are engaging in similar traffic shaping practices for the stated purpose of optimizing network operations**.** In Canada, Rogers Communications Inc. has been the subject of many user complaints about its traffic shaping practices, even before Bell began engaging in similar practices.[14] Other Canadian ISPs who have been accused of engaging in this practice include Shaw Communications, Cogeco, and

---

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

[11] Bell Canada, *In the Matter of an Application by Canadian Association of Internet Providers Pursuant to Part VII of the CRTC Telecommunications Rules of Procedure and Sections 7, 24, 25, 27, 32, 36 and 62 of the* Telecommunications Act *Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" its Wholesale ADSL Access Services: Answer to Request for Interim Relief* (15 April 2008) [Bell Answer] at ¶16.

[12] *Ibid*. at ¶14.

[13] CAIP Letter, *supra* note 1, Exhibit C (being a single-page letter from Bells' Senior Vice president Carrier Services to Bell Canada's ISP Customers).

[14] See http://www.azureuswiki.com/index.php/Bad_ISPs#Canada; http://www.ottawabusinessjournal.com/319629855570564.php;

Eastlink. We believe that these Company's practices also merit investigation for compliance with PIPEDA.

16. Bell has become the subject of recent complaints largely because it began applying traffic management practices to wholesale internet services, not just retail services, thus affecting customers of other ISPs as well as its own customers.

17. Bell says that its Internet traffic management technique relies in part on "deep packet inspection" that it applies to "P2P file sharing and bit torrent applications…."[15] It has not provided any details about how it undertakes or applies DPI, but has said that "it only looks at the application header of the content but not the content itself, and it does not block access to any content or applications."[16]

18. Bell has denied that its use of DPI affects end-users' privacy. In its Answer to the CAIP Application, Bell asserts the following:

> **Not affecting end-user's privacy nor controlling the content or influencing the meaning or purpose of telecommunications under s. 36:**
>
> 41. As noted above, the Company's use of DPI as part of its Internet traffic management solution is such that it treats all P2P traffic the same and it only looks at the application header of the content but not the content itself. As part of its traffic management solution, the Company does not block access to any content or applications. Therefore, the Company is not affecting end-user's privacy nor is it controlling the content of influencing the meaning or purpose of telecommunications. As explained in more detail in Appendix 1, the DPI equipment used by Bell does not retain the information that it has reviewed from the packet headers and the content itself is not actually reviewed, analyzed or stored. Furthermore, it is also common knowledge that other Canadian ISPs also [sic] similar technologies in their networks to manage traffic.[17]

19. Bell's Chief of Regulatory Affairs recently told *The Gazette* that Bell is focused on heavy users of P2P and that it is

> … not targeting particular people or particular content, we're directing these measures at a particular type of traffic. It's not slowing down peer-to-peer for everyone. … It's actually the P2P by heavy users, whether or not they're on Sympatico or on the wholesale ISP. And at that, it's only during so-called peak periods. Those who use P2P to a reasonable degree are not affected.[18]

---

15 CAIP letter, *supra* note 1, Exhibit C (being a single-page letter from Bells' Senior Vice president Carrier Services to Bell Canada's ISP Customers).

16 Bell Answer, *supra* note 14 at ¶8.

17 Bell Answer, *supra* note 14 at ¶41 [underlining added].

18 Roberto Rocha, "Internet throttling defended: 'Resellers don't want to invest anything'" *The Gazette* (11 April 2008) [Internet throttling].

20. In its Reply to Bell, CAIP disputes Bell's claim that it does not examine the content of traffic packets, noting that "the literature on DPI does not support these assertions."[19]

21. 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 Bell's practices, involve the inspection and differential treatment of internet traffic. The FCC is expected to rule on the matter by June 30th. Comcast 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.[20]

22. 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".[21]

II APPLICATION OF PIPEDA TO BELL'S USE OF DPI

Deep Packet Inspection involves the collection and use of "personal information"

23. 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.[22] Information about

---

19 CAIP, *Reply* (24 April 2008) at 68.

20 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>.

21 Todd Spangler, "Comcast Pledges to Help Bittorrent, not Hinder it", Multichannel News, 3/27/2008.

22 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>.

data packets gathered by ISPs through the use of DPI are (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.

24. The evidence is clear that DPI technologies permit the collection and use of personal data about internet subscribers. The extent to which Bell 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 tool for ISPs.

25. If Bell 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 Bell (and other ISPs) to use DPI to distinguish among traffic in ways that necessarily involve the collection and use of personal data.

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.*

26. As noted above, Bell is using DPI to manage traffic not only of its own retail customers but also of end-users who are customers of Bell's wholesale ISP customers. As Bell has no contractual relationship with these end-users, it cannot obtain their consent to the inspection of their traffic. We therefore submit that Bell is in violation of PIPEDA's consent requirement at least in respect of those affected internet users who are not customers of Bell.

27. Even with respect to its own customers, however, Bell is failing to obtain informed consent to this practice. Not only is it difficult for endusers to find the company's *Bell Customer Privacy Policy*, but neither that policy nor any of the other privacy documents or statements to which Bell directs its customers actually refer to Bell's practice of linking identifiable subscribers with specific data packets.

28. Insofar as Bell's own Sympatico customers are concerned, Sympatico's *Terms of Service*[23] stipulate that when customers first use the Sympatico Network they agree to be bound by the *Terms*.[24] The *Terms* advise that Bell may monitor the Sympatico network to operate it "properly", but not that Bell may monitor the Internet *activities* of individual subscribers for this purpose. Specifically, the Terms state that:

> … Sympatico has the right to monitor the Sympatico Network electronically from time to time and to disclose any information as necessary to satisfy any law, regulation or other governmental request, to operate the Sympatico Network or any of the Services properly, or to protect itself or its users in accordance with **Sympatico's Privacy Policy**. …
>
> Section 6 ("Monitoring", bold font added)

29. The *Terms* then state that Sympatico may "protect itself" in accordance with Sympatico's *Privacy Policy*, to which a link is provided in section 2. This link did not work when we tried it on 9 May, 2008; instead, it redirected us to the Bell "Internet customer support centre", from which there was no other link to the full *Privacy Policy*. We were thus unable to locate a copy of Bell Sympatico's full *Privacy Policy*.

30. In our review of Bell's privacy policies during the week of 5 May, however, we were able to access the *Bell Customer Privacy Policy* dated "00 09 07" (see attached). This *Privacy Policy* defines personal information as "information about an identifiable individual. This includes information about your product and service subscriptions and usage. Publicly available information, such as a public directory listing of your name, address, telephone number, electronic address, is not considered to be personal information" (p. 3). It then sets out six broad purposes for which the Bell companies collect personal information, none of which refer to the linking of identifiable subscribers with specific data packets:

---

[23] *Sympatico Network Terms and Conditions*, online: Sympatico.ca <http://www1.sympatico.ca/About_Us/terms.html> accessed 6 May 2008.

[24] *Ibid*. at s. 7:

> …
> **By accessing the Sympatico Network or using any of the Services, you agree**, without limitation or qualification, **to be bound by these terms and conditions** and such other additional or alternative terms, conditions, rules and policies which are displayed or to which you may be directed in connection with any particular Service or any Sympatico Network web site, as all of the same may be modified by Sympatico from time to time (collectively the "Terms and Conditions"). Please note that the Terms and Conditions may be updated from time to time without notice to you, so please check back periodically. The most current version of the Terms and Conditions can be found at http://www1.sympatico.ca/About_Us/terms.html.
> (bold font added)

- to establish and maintain responsible commercial relations with you and provide you with ongoing service;
- to understand your needs and eligibility for products & services;
- to recommend particular products & services to meet your needs;
- to develop, enhance, market or provide products and services;
- to manage and develop Bell's business and operations, including personnel and employment matters; and
- to meet legal and regulatory requirements.

The *Customer Privacy Policy* goes on to say that "Your personal information will not be used for any other purpose without your consent" (page 4).

31. Instead of links to the full Bell Sympatico *Privacy Policy*, the "Bell Security & Privacy Policy"[25] page provides links to: a short form of Bell's Privacy Policy called the *Bell Privacy Statement*, Bell's *Code of Fair Information Practices*, and "the Bell Privacy FAQs". [26]

32. We note that by this time in their visit to Bell's website, end-users interested in learning about Bell's privacy commitments will be presented with the option of consulting at least three separate documents, not to mention the missing full version of Bell's *Customer Privacy Policy*. This approach to informing end-users about their privacy rights, in our view, meets neither PIPEDA's "readily available" nor its "without unreasonable effort" requirements under Principle 4.8, let alone the requirement for informed consent under Principle 4.3.

33. The *Bell Privacy Statement*[27] is a one-page document that defines personal information as "information about an identifiable individual. This includes information about your product and service subscriptions and usage." The *Privacy Statement* sets out five broad purposes for which it collects, uses and discloses personal information, none of which refers to DPI or the linking of data packets to identifiable subscribers:

- To establish responsible relations with you and provide you with ongoing, quality service
- To understand your needs and preferences
- To recommend particular products and services to meet your needs and determine your eligibility for certain other products & services

---

[25] "Bell commitment to privacy", online: Bell.ca <http://www.bell.ca/support/PrsCSrvGnl_Privacy.page?language=en&region=ON&selecteddropdown=0>. The Bell commitment to privacy

[26] Bell, *Privacy: The Bell commitment to privacy*, online: Bell.ca <http://www.bell.ca/support/PrsCSrvGnl_Privacy.page?language=en&region=ON&selecteddropdown=0>.

[27] *Bell Privacy Statement*, online: Bell.ca <http://www.bell.ca/web/common/en/all_regions/pdf/shortform_privacy.pdf>.

- To develop, enhance, market, or provide products and services
- To meet legal and regulatory requirements

34. The Bell *Code of Fair Information Practices*[28] defines personal information broadly as "information about an identifiable individual but not aggregated information that cannot be associated with a specific individual." ("Definitions"). The *Code* sets out five purposes for which the Bell companies collect personal information, none of which refers to DPI or the practice of linking identifiable subscribers to specific data packets:

> a) To establish and maintain responsible commercial relations with customers and to provide ongoing service;
>
> b) To understand customer needs;
>
> c) To develop, enhance, market or provide products or services;
>
> d) To manage and develop their business and operations, including personnel and empl9oyment matters; and
>
> e) To meet legal and regulatory requirements.

35. Another link on the "Bell Security & Privacy Policy" page[29] directs visitors to Bell Privacy FAQs.[30] Frequently asked question 3 ("**What are the purposes for collecting personal information?**") sets out the purposes for which the "Bell Companies" (*i.e.*, not just Sympatico) collect information when they provide service. While these purposes include Bell's monitoring of "usage volumes", the FAQ does not refer to the linking of identifiable subscribers with specific data packets:

> **The Bell Companies collect information** during the application process, when communicating or transacting business with you, and **when providing you with service**. We also collect information about you from third parties that have the right to disclose such information to us.
>
> The Bell Companies collect information only for the following purposes:
>
> - To establish and maintain responsible commercial relations with you and provide you with on-going service;
>
> *For example, we may collect information to confirm your identify or to establish credit worthiness.*
>
> - To understand your needs and preferences and to determine your eligibility for products and services;
>
> *We retain records of your purchases and your use of Bell products and services and may ask you, from time to time, for additional information to serve you better such as an eMail address to quickly send you help desk and user guide information.*
>
> - To recommend particular products & services to meet your needs;

---

[28] Bell, *Code of Fair Information Practices*, online: Bell.ca <http://www.bell.ca/web/common/en/all_regions/pdfs/bcfip.pdf>.

[29] *Supra*, note 26 (Bell commitment to privacy).

[30] Bell, Privacy FAQs, online: Bell.ca <http://www.bell.ca/support/PrsCSrvGnl_Privacyfaq.page>.

We may periodically review your product and service profile in order to determine if other Bell products and services might better meet your needs. For example, if you currently subscribe to 2 or more Bell lines of business, you may be eligible for service bundle savings.

- To develop, enhance, market or provide our products and services;

  We continually review and analyze customer use and purchase behaviour in order to ensure that our products and services respond to customer needs and desires.

- To manage and develop Bell's business and operations, including personnel and employment matters;

  *For example, **we monitor usage volumes** in order to plan and provision our communications networks and product sales results and to determine the success of features, promotions and pricing.*

- To meet legal and regulatory requirements.

  For example, we may be required to collect information by a court order or to demonstrate compliance with a CRTC requirement.

Your personal information will not be used for any other purpose without your consent.[31]

36. To summarize, neither Bell's *Terms of Service*, its *Privacy Statement,* its *Code of Fair Information Practices,* nor its FAQs disclose Bell's alleged practice of inspecting data packets that are or can be linked to identifiable individuals, for traffic management or other purposes.

37. Consent is only meaningful when affected individuals understand what they are consenting to. If Bell 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*.

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.*

38. Even if Bell were to have obtained informed consent from its subscribers and the subscribers of other affected ISPs to its use of DPI, however, the evidence suggests that Bell can manage its network adequately without inspecting the content of user communications.

---

[31] <http://www.bell.ca/support/PrsCSrvGnl_Privacyfaq.page>

39. First, other ISPs whose networks are based on the same basic technology as Bell's (e.g., TELUS Communications, MTS/Allstream and SaskTel) do not, apparently, engage in this practice.

40. Second, 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".[32]

41. Third, Bell 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.

42. Fourth, there are other, less privacy invasive, means for Bell 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 Bell 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.

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

---

[32] Todd Spangler, "Comcast Pledges to Help Bittorrent, not Hinder it", Multichannel News, 3/27/2008.

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.*

44. As noted above, neither Bell's *Terms of Service*, its *Privacy Statement,* its *Code of Fair Information Practices,* nor its FAQs state that Bell will use Sympatico subscribers' personal information to examine 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, Bell Sympatico's *Privacy Policy* - the document that people consult in order to understand Bell's practices regarding the collection, use and disclosure of personal data - does not provide any specific references to or information about its use of DPI.

45. Bell 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 purposes.

III. REQUEST FOR INVESTIGATION AND FINDING

46. On the basis of the above allegations, we request that you investigate Bell's use of DPI for traffic management purposes with a view to its compliance with *PIPEDA*.

47. 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 ISPs (in particular, Rogers, Shaw, Cogeco, and Eastlink), not just Bell.

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

Yours truly,

Philippa Lawson

Attachments