

**Office of the
Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

**Commissariat
à la protection de
la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télec.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



File: 6100-03063

AOUT 13 2009
AUG 13 2009

Mr. David Fewer
Acting Director
Canadian Internet Policy and Public Interest Clinic
University of Ottawa
Faculty of Law
57 Louis-Pasteur
Ottawa ON K1N 6N5

Dear Mr. Fewer:

Please find attached the report of findings prepared by this Office with regard to the complaint you filed against Bell Sympatico under the *Personal Information Protection and Electronic Documents Act*, and received by our Office on May 12, 2008.

Following the investigation into your complaint, I have concluded that the matter is partially well-founded. For details on the investigation and the rationale for my conclusion, please see the attached report of findings.

Now that you have my report, I must inform you that, pursuant to section 14 of the *Act*, you have the legal right to apply to the Federal Court of Canada if you wish to pursue this matter any further.

Should you wish to proceed to Court, we suggest you contact the Court office nearest you. Normally, an application must be made within 45 days of the date of this letter. For additional information on Federal Court applications, please check the Fact Sheet, Application for Court Hearings under PIPEDA, found on this Office's web site at http://www.privcom.gc.ca/fs-fi/02_05_d_31_e.asp.

This concludes this Office's investigation of your complaint. If you have any questions or comments about the disposition of the complaint, I would invite you to contact Jolana Klobouk, Privacy Investigator, at 1-800-282-1376.

Sincerely,

A handwritten signature in black ink, appearing to read 'Elizabeth Denham'.

Elizabeth Denham
Assistant Privacy Commissioner

Attachment



Report of Findings

File 6100-03063

Complaint under the *Personal Information Protection and Electronic Documents Act (the Act)*

1. The complainant alleges that Bell Sympatico (Bell) uses Deep Packet Inspection (DPI) technology during Internet transmissions to collect and use personal information from its customers without their consent.
2. The complainant also claims that this practice collects more personal information than is necessary to fulfill the company's stated purposes of ensuring network integrity and quality of service.
3. The complainant alleges as well that Bell does not adequately inform its customers of its practices and policies concerning the collection of their personal information during Internet transmissions.

Summary of Investigation

Overview: What is DPI and how is it used?

4. DPI is a tool used by Internet service providers (ISPs) to view information transmitted on the Internet (e.g. from e-mails, downloads, uploads) in order to manage the ISPs' network traffic.
5. Information is transmitted via the Internet using a protocol that breaks information into packets, routes that information to its destination and reassembles the information in the packets into the original content. The content (or "payload") is the user-generated information (such as e-mail content) that is surrounded by several layers of control information to ensure proper handling and routing.
6. DPI has the capacity to see through and inspect these many protocol layers. For example, viewing down to the application layer of a packet—the layer directly above the payload—allows an ISP to determine the type of software application that is being used to transmit the packet. Depending on the particular method that an ISP adopts, being able to isolate and identify application information can be useful to the ISP's ability to manage its network traffic and reduce the traffic congestion that its clients can experience on the Internet. Some software applications are heavy users of bandwidth and are designed to use available



capacity in the network in order to transmit their information. E-mail is typically a small consumer of bandwidth, while the file sharing and Peer-to-Peer (P2P) applications are large users. Applications that are often used for music and movie file sharing between computers can consume a great deal of capacity and “slow down” other Internet traffic.

7. Each packet layer also has its own header, one of its functions being a marker that identifies the layer and differentiates it from all surrounding layers. These headers are sometimes referred to as “protocol headers”.
8. DPI cannot be considered new technology. DPI has been used in the past as the integral part of an intrusion prevention system, an intrusion detection system or with traditional firewall technology. Thus, DPI can be beneficial to a user as a security aid. What is new, however, is how it is currently being employed by Bell and other ISPs in traffic management.

Why does Bell deem it necessary to use DPI?

9. In its representations, Bell claims that the amount of traffic specifically using Peer-to-Peer (P2P) applications is causing undue congestion on its network; this represents a threat to the network and degrades Internet service to its clients by slowing service, especially during peak Internet usage periods.
10. Bell contends that its use of DPI as part of its Internet traffic-management solution to congestion problems during peak periods has been restricted to targeting only P2P file-sharing applications. According to Bell, peak periods occur between 4:30 p.m. and 2:00 a.m. During this time, the upload and download rates of speed for P2P transmissions are gradually decreased at the beginning of the period and then gradually increased towards the end of a peak period.
11. This Office’s investigation confirmed that the use of P2P applications to transmit content through the Internet does increase network traffic (i.e. consume more bandwidth) than other client-server applications and that the widespread phenomenon of congestion in networks is largely caused by user downloads or computer-to-computer file sharing using P2P applications. Relying on traffic-management tools such as DPI is one means, among several, by which ISPs can optimize network traffic flow.



Who is targeted by Bell's use of DPI?

12. Bell advised that it carries Internet traffic for its Sympatico subscribers, as well as Internet traffic on a wholesale basis for smaller competing ISPs, and that the traffic of both Sympatico and wholesale customers has been subject to traffic management using DPI.

What can DPI examine?

13. According to the complainant, DPI is also able to examine the user-generated content of a data packet. One source that the complainant cites names a firm that purportedly uses DPI to look inside packets and reassemble fragmented information. In so doing, the firm can re-create from Internet traffic a readable record of e-mails, web browsing activity, Voice-over-Internet protocol (VoIP) calls and passwords.
14. The complainant also cites a news release of another firm, involved in the designing of traffic-management tools based on DPI technology. The news release informs how its own product provides "...reports on subscriber and application usage to enable effective service marketing based on real subscriber behavior data." An industry analyst is quoted as saying that "...this kind of technology can provide an invaluable tool for marketing executives."
15. Our investigation was able to confirm that DPI can examine the following:
- Most popular services or applications (P2P, VoIP, on-line games, e-mail, video...)
 - Subscriber usage patterns (by using the Internet Protocol [IP] address of a computer)
 - Application usage patterns
 - Competing services and their presence on the network (e.g. amount of VoIP traffic)
 - Malicious traffic on the network



16. Moreover, although DPI was designed to look within the application header of a packet or traffic stream, our investigation confirmed that it is possible to use certain DPI technology to look further and examine the payloads of packets being sent (e.g. e-mail, on-line games, video). This content can contain personal information, such as photo images, and financial and contact information.

How does Bell use DPI?

17. Bell stressed that its use of DPI does not extend to other applications (e.g. streaming applications such as Internet radio or YouTube).
18. Our investigation examined, in detail, Bell's submission to the Canadian Radio-Television and Telecommunications Commission (CRTC). It made the following claims:

By design, the DPI devices deployed in Bell Canada's network **do not**:

- use any personal identification information of an individual user;
- store or log any personally identifiable information;
- have specific knowledge of a user's real identity;
- have knowledge of a user's URL browsing history;
- have knowledge of a user's Internet search activity;
- have knowledge of a user's email topics or content;
- store content accessed by a user;
- cache any content, including user-specific content, whatsoever;
- capture and playback any communications exchange; or install or require any specific software on user machines

19. In its representations, Bell claims that the DPI devices deployed in its network are not configured to distinguish types of customer content contained in packets. Bell asserts that it is not using DPI for user-generated content inspection, but rather for flow classification.



20. In a report filed with the CRTC, Bell acknowledges that the DPI technology it uses on its network has the capability to inspect content, but that it does not use it for this purpose. The report states the following:

However, Bell Canada could configure a specific filter, to match a specific value at a specific packet offset in order to isolate a specific communication exchange. But this information would have to be known prior by Bell Canada in order to set the specific fields and offsets to match. This type of filter could likely be placed on any network element, not just DPI. The Company is not introducing any such configurations as part of its traffic management solution.

What is an IP address?

21. An IP address (also called an Internet address) is a unique numeric address (e.g. 1.237.10.591) that identifies a specific computer on a network, such as on the Internet. When information is transmitted on the Internet, the respective IP addresses of the sender and the receiver are included in each packet. While a static IP address constantly identifies the same computer throughout different logon sessions on a network, a *dynamic* IP address is one that can change with each new logon session from the same computer, thereby introducing elements of randomness and relative anonymity. Yet random as they may appear to be, dynamic IP addresses are often associated with an invariable identifier, such as a subscriber's user ID (conferred by the ISP), which, depending upon the ISP and its information systems, can be traced back to an individual ISP subscriber.

How are IP addresses handled when Bell uses DPI?

22. In the report from Bell to the CRTC, the respondent also describes how IP addresses are handled when Bell uses DPI. It first explains how, on a network, several information packets are grouped into a "flow" during transmission and how DPI then parses information from packet headers and stores the information in a "flow table". A diagram of the flow table clearly indicates that, during this process, both the sender's and receiver's IP addresses are stored by DPI in the flow table.
23. Later in the report, Bell reinforces this by stating that, "The DPI technology deployed by Bell Canada has the ability to identify the source IP address and the destination IP address of both the sender and the receiver of the communications exchanges, when creating and managing flows."



24. The report states that its normal operations of DPI allow it to identify the IP addresses of traffic only on its access network: "On its own...the DPI can identify either the IP address of a sender or a receiver when they are on the Bell Canada access network, but not when they are on the Internet." Thus, it would appear that the user IP addresses that can be identified by Bell would comprise at least those of its own subscribers. Accordingly, the IP addresses of non-subscribers (i.e. having a different ISP) can also be identified by Bell if the non-subscriber's message uses Bell's access network during its transmission from sender to receiver (e.g. a message sent from a Sympatico non-subscriber to a Sympatico subscriber).

25. Bell goes on in the report to explain that the capability also exists for a wider application:

This normal operation of the DPI can be overridden with a configured destination-specific filter, which can be used to establish flows with any IP source IP address going to a filter-specific destination IP address (fully-qualified 32-bit IP address). This would require Bell Canada to configure the specific destination IP address for any flows it wanted to be processed matching the filter.

26. This application could include inspection of user-generated content:

The DPI does theoretically have the technical feasibility of assigning a filter on a specific location in the packet payload, i.e. the actual content ...However, this application would be very impractical since the current Bell Canada architecture and design is not tailored for this type of use.

27. Bell further explains that its subscribers are assigned dynamic IP addresses while using its network, although each assigned user ID remains constant. In this way, a specific user ID, while logged on to the Bell network, can be assigned several different IP addresses, each corresponding to different periods of time the user spends on the network:

The closest identifier to an individual subscriber that the DPI currently does maintain and store is a 'subscriber id' which is actually Bell Canada's user ID assigned by network authentication in order to bind a user to an assigned IP address. ...the DPI is capable of identifying network users and associating dynamic IP addresses that have been assigned to each user. Often, IP addresses are assigned dynamically in order to accurately account for usage billing.



28. Bell contends that, in this way the person using the network is not uniquely identified—only their “customer premises device” (e.g. computer or router) is identified—and that “While there is no capability for the DPI device itself to resolve [i.e. to link] an IP address to a specific human user of the network, this information may be used by Bell Canada for purposes of bandwidth consumption management, e.g. if a customer has a specific Internet access service plan with a bandwidth cap.”

What are Sympatico customers informed of and are they allowed an opportunity to consent?

29. Bell confirmed to this Office that it began using DPI on its Sympatico customers in late 2007. Our investigation did not reveal any evidence to show that Sympatico customers were advised by Bell that their traffic would be subject to inspection. However, according to the complainant, Bell informed some of its wholesale ISPs on March 28, 2008, that it had begun using traffic-management measures on Sympatico customers.
30. This Office's examination of the Bell Internet Service Agreement and the Bell Internet Dial-up Service Agreement (both updated August 11, 2008 and available on the company website) indicated that users are informed in a general way of the possibility of Bell monitoring their use of Bell's networks. Specifically, paragraph 17 (User Information: Other Information) states, in part, the following:

... However, you agree that Your Service Provider reserves the right from time to time to monitor the Service electronically, monitor or investigate Content or your use of Your Service Provider's networks, including, without limitation, bandwidth consumption, and to disclose any information necessary to satisfy any laws, regulations or other governmental request from any applicable jurisdiction, or as necessary to operate the Service or to protect itself or others.

31. Paragraph 17 continues:

You hereby acknowledge that Your Service Provider, its affiliates, agents and suppliers may retain and use any information, comments or ideas conveyed by you relating to the Service (including any products and services made available on the Service). This information may be used to provide you with better service.

32. Bell contends that the information about its practices that it has made available for customer consent purposes is sufficient and that an organization's obligation to collect, use or disclose personal information under the *Act* excludes it having to “...explain the specific technology that it uses to do so or that it obtain consent for the use of specific technology....”



33. It further states (using the example of its practice of recording calls to 310-BELL for quality-assurance purposes) that it is also not obliged to inform individuals of the existing capabilities of the technology it uses nor of all the possible future uses. However, the respondent acknowledges that if it were to use the call-recording technology in the future "... for a different purpose, e.g. marketing purposes, it would have to do so in compliance with the PIPEDA obligations, such that a new purpose would have to be identified, consent ... would have to be obtained prior to doing so and the form of consent would depend on the sensitivity of the information. No consent would be sought on the actual technology being used to do so."
34. Relating specifically to DPI technology, Bell affirms that its use of DPI for purposes other than those it currently identifies "...would be made in accordance with Bell's PIPEDA privacy obligations, our privacy policies and applicable customer agreements."

How else are its customers or the general public informed of Bell's monitoring and traffic-management activities?

35. The complainant claims that there is a lack of clarity and coherence in information available on Bell's websites relating to its network monitoring policies and practices. For example, on the company website, part of the Bell's Terms of Service document refers readers to the Sympatico Privacy Policy. However, the complainant alleged that the link between the web pages was broken.
36. During our investigation, this Office was informed by Bell that the Sympatico Privacy Policy document no longer exists, having been replaced instead by Bell's Code of Fair Information Practices and an abbreviated, one-page privacy statement. Bell also confirmed that the alleged broken link to the former privacy policy had been repaired and that the content of the web page was updated. Instead, Bell now advises that customers should refer to the permanent privacy link available at the bottom of every web page in order to find relevant privacy policies.
37. Our investigation determined that the documents relevant to privacy and Bell's Internet service are now the following: Bell Code of Fair Information Practices (the Code); Frequently Asked Questions (FAQs); Privacy Statement; Bell Internet Service Agreement, Bell Internet Optimax Service Agreement and Bell Internet Dial-up Service Agreement. By clicking on the privacy link from any Bell web page, an individual gains access to the privacy page, which provides links to the Code, the FAQs and the Privacy Statement.



38. In the FAQs, question #12 ("Does Bell Sympatico monitor my service?") advises that Bell can monitor aspects of a subscriber's use:

Bell Sympatico does not proactively monitor your use of the Service or the content of your emails.

However, Bell Sympatico, similar to other Internet service providers, reserves the right from time to time to monitor the service electronically. In the normal course of business, Bell Sympatico may be required to monitor certain aspects of your use of the Service, such as your bandwidth consumption or spamming in order to ensure the operation of the Service, or to ensure compliance with other provisions of our Acceptable Use Policy such as the harassment of other users, uploading, downloading....

At this FAQ, Bell provides a link to the three Internet user agreements, where the Acceptable Use Policy can also be found.

39. Even though in its representations dated July 15, 2008, Bell claims it was working on "...the addition of a specific FAQ for its use of DPI technology for such purposes [i.e. traffic-management measures] ...", we note that such a question has not been added to the FAQs page as of the issue date of this report of investigation.
40. Specific information about how and why Bell uses DPI is available on the company website (www.bell.ca) in the form of questions and answers, to be found under the heading "Network management", when one follows the following links: Home/Support/Internet/troubleshooting/slow connection/Network management. We noted that there is no direct link provided from the FAQs or other privacy- or user-related documents to this information. The response to the final question, "Is Bell allowed to do this?", is given as follows and specifically refers readers to the Internet service agreement:

Bell has a responsibility to maximize the ability for all customers to use and enjoy their Bell Internet service and a responsibility to deliver bandwidth fairly to its customers

In order to fulfill these responsibilities, Bell is entitled under the terms of the Service Agreement to utilize the technology that maintains or enhances the performance of the Service and the integrity of the network.



Application

41. In making our determinations, we applied Principle 4.3, which states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Personal information is defined in section 2(1) as information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.
42. Principle 4.3.2 adds that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
43. We also applied Principle 4.4, which stipulates that the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means
44. Finally, we applied Principle 4.8, which states that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Findings

45. On April 24, 2009, I issued a report of investigation, in which I noted that Bell's actions were not in compliance with various provisions of PIPEDA and I made four recommendations to Bell, with the view of helping the organization meet its obligations. Bell responded to the recommendations.
46. What follows is the original text from the report of investigation:
47. At issue in the first place is whether any information that Bell is collecting or using for the purposes of DPI can be considered personal information. This Office has previously found that an IP address can constitute personal information if it can be associated with an identifiable individual. Further, our investigation has established that, to manage network traffic, Bell's DPI devices as currently configured, collect and use the following information relating to a given communication:
 - IP addresses;
 - Subscriber id/User Identifier pertaining to Bell customers; and
 - Application type



48. We ascertained from our investigation that Bell assigns its subscribers a dynamic IP address when a Sympatico subscriber connects to the network. Bell has indicated that it binds each dynamic IP address to an invariable “subscriber id” that can be traced back to an individual Sympatico subscriber. In this way, Bell can determine which Sympatico subscriber is associated with a dynamic IP address at a given time. Given that Bell can link its Sympatico subscribers, by virtue of their subscriber ID, with Internet activities (in this case, type of application being used) associated with their assigned IP addresses, in my view, IP addresses in this context are personal information.
49. We have not seen any evidence to indicate that Bell can link IP addresses not associated with Sympatico subscribers with an identifiable subscriber. Therefore, in the circumstances, Bell cannot be said to be collecting or using personal information with respect to IP addresses belonging to non-Sympatico subscribers.

Knowledge and Consent

50. In the first paragraph of clause 17 of the Bell Internet Service Agreement and the Bell Internet Dial-up Service Agreement, Bell’s own subscribers are advised that their use of Bell’s networks, as well as content, may be monitored by the service provider. In my view, after reading this part of the agreement, one would reasonably expect that some personal information could be monitored. Therefore, the general provisions of Principle 4.3 would appear to be met.
51. However, the matters of whether individuals are clearly informed of the specific purposes of the uses of their personal information, provide meaningful consent and are clearly informed of the specific purposes of the uses of their personal information—as required by Principle 4.3.2—are more problematic. For example, the text of the second paragraph of clause 17 refers to the retaining and using of information by several parties other than Bell (e.g. “affiliates, agents and suppliers”), followed by an open-ended description of the types of information to be retained and used by these parties. When combined with the stated, broad purpose for the retaining and using of the information (“...to provide you with better service”), the end result is a less than meaningful message from which, in my view, average individuals would not be able to reasonably understand how their personal information could be used or disclosed. In this regard, I find that the requirements of Principle 4.3.2 have not been met. Moreover, it is not clear to what extent the second paragraph of clause 17 is meant to relate to Bell’s use of DPI. This is problematic given that Bell’s stated uses of DPI do not include disclosures of personal information to third parties.



52. While Bell's stated purpose for using DPI is currently restricted, Bell has asserted that any added uses for DPI would respect the applicable customer agreements. Clause 17 of Bell's Internet Service Agreement and the Bell Internet Dial-up Service Agreement states that the respondent reserves the right to "... monitor or investigate Content...". Such a provision in the service agreements, in addition to the statements regarding disclosures of personal information noted above in paragraph forty-nine, could theoretically be relied upon by Bell to expand its current uses of DPI without seeking the express consent of users.
53. However, in my view, clause 17 is not sufficiently informative such that customers would be able to provide meaningful consent to expanded uses of DPI under this rubric. Therefore, reliance on clause 17 to support expanded uses of DPI would be contrary to the *Act*. As such, I would expect that Bell would not engage in any expanded uses of DPI without taking steps to clearly inform its customers.

Limited Collection

54. At issue in the third place is, relative to Principle 4.4, whether more information than necessary is being collected for the purpose of ensuring network integrity and quality of service. In my view, managing network traffic by targeting P2P file-sharing applications in order to ensure adequate bandwidth and quality of Internet service for its customers is an acceptable business purpose for an ISP.
55. I am unconvinced that, at date of issue of this report, Bell is collecting or using any personal information of individuals other than the IP addresses and subscriber IDs of Sympatico customers when it uses its DPI technology for the purpose of network traffic management. For this reason, Principle 4.4 has not been contravened.
56. Nonetheless, I am aware that DPI platforms have the capability to allow an organization to view information of a potentially very sensitive nature—for potentially different purposes and if the organization were to apply the proper configurations. Bell has stated that the DPI platform it uses has this capability, but that it is currently not using it for this purpose. It has also assured this Office that any added purposes for which it currently uses DPI would respect the company's privacy obligations under the *Act*, its own privacy policies and applicable customer agreements.



Openness

57. Lastly, relative to Principle 4.8, is whether Bell adequately informs its customers of its policies and practices concerning the collection and use of their personal information when the company uses DPI.
58. I have several specific concerns in this regard. To begin with, the information that Bell makes available to its customers regarding its traffic management practices and the use of their personal information for this purpose is presented in a fragmented and not readily available manner on the company website. Rather than being integrated into its "Privacy" link appearing on each website page, crucial information about the management of personal information is fragmented and spread out over three separate sources: FAQ #12, the service agreements and the relatively obscure "Network Management" web page. The most informative of these sources for customer consent purposes are the latter two, but they are also the least readily available. As well, there exists no FAQ pertaining to Bell's use of DPI technology for traffic management.
59. Bell's answer to the question "What is Deep Packet Inspection (DPI) and what does it have to do with Internet traffic management?", located on its "Network management" web page is not accurate. Our investigation revealed that through DPI, Bell collects IP addresses and can associate them with a subscriber id for its own Sympatico subscribers; in my view, this is "personal information".
60. Therefore, pursuant to the provisions of the *Act*, all information from Bell about the extent of and purposes for its traffic management practices should be accurate, understandable, integrated and more readily available. Until these problems are corrected, Principle 4.8 will not be upheld.

RECOMMENDATIONS FROM REPORT OF INVESTIGATION

61. In my report of investigation, I made the following recommendations with regard to openness:
- i. That Bell clarify the extent to which the second paragraph of clause 17 of the Internet service agreements relates to Bell's traffic management practices;
 - ii. That Bell integrate Bell's policies and practices (on the website and in printed form) about its traffic management into one format that is accurate as well as easily identifiable, retrievable and understandable;



- iii. That Bell develop and add an explanatory Privacy FAQ about Bell's traffic management practices and the privacy impact on customers;
- iv. That Bell revise the answer to the question "What is Deep Packet Inspection (DPI) and what does it have to do with Internet traffic management?", found on Bell's "Network Management" web page. The answer should state that personal information is collected.

BELL'S RESPONSES TO RECOMMENDATIONS

62. Bell responded to our recommendations.
63. Firstly, concerning our recommendation to clarify the second paragraph of clause 17 of the *Bell Internet Service Agreement* (clause 14 of the *Bell Internet Dial-up Service Agreement*), Bell confirmed that this part of the clause does not relate to its traffic management practices. Rather, Bell states that it applies to comments that subscribers may make about the service on Bell bulletin boards or in online forums, for example. Nevertheless, I am requesting that Bell better indicate to users what this part of the clause refers to, by adding an underlined heading (e.g., "Customer Service Information") at the beginning of the second paragraph of this clause. We will be following up with Bell within 30 days to verify the status of this request.
64. Secondly, with regard to our recommendation that Bell revise how it organizes and displays on its website and in printed form its policies and practices on traffic management, the organization responded that all information on its traffic management policies is found at one URL ("Network Management"): http://service.sympatico.ca/index.cfm?method=content.view&content_id=12119. Further, Bell advised that this URL can be accessed by users in several ways from the home page www.bell.ca. ("e.g. search function, 'Customer Commitment' link at the bottom of every page, 'My Internet Usage' page"). In this sense, Principle 4.8 has been upheld.
65. Thirdly, in response to our recommendation to develop and add a FAQ about Bell's traffic management practices and the privacy impact on customers, Bell responded that it intends to add a FAQ at www.bell.ca/privacy when the outcome of the current complaint is made known. Accordingly, Bell has proposed a draft FAQ and an answer to it. I have reviewed this draft and am recommending a further revision to the answer. In my view, the answer does not fully address and inform how the traffic management practices impact the privacy of users, specifically with regard to the collection of IP address, which we deem to be personal information in the case of Sympatico subscribers.



66. That being said, in the draft answer to the FAQ, I note approvingly that there is a direct link to the "Network Management" URL; this is an essential gateway, directing individuals who begin their website search of DPI from the perspective of user privacy to more precise information about the organization's use of DPI (from a network performance perspective). The bridging of these two URLs also responds to our second recommendation, that of improving the overall organization and display of information on this topic available from the Bell website.
67. Concerning our fourth recommendation, which was for Bell to revise the answer to the question "What is Deep Packet Inspection (DPI) and what does it have to do with Internet traffic management?" (from the "Network Management" URL), so as to indicate that the personal information of Sympatico subscribers is collected in the form of an IP address, Bell has not complied. While Bell acknowledges that it uses IP addresses and links them to subscriber user IDs, for network congestion management purposes, it considers that the brevity of the traffic management process results in there being "...no 'collection' per se of the IP addresses linked to the subscriber user IDs in this particular context." Bell offers further that the IP addresses are "... not retained or stored longer than necessary to apply the particular traffic management policy" and also that "... at no time can Bell look up a subscriber's account and know whether their P2P file sharing application was being shaped at any given time."
68. In my view, Bell collects and uses the IP addresses. However, we have no evidence to believe that they are retained after they are no longer needed for the purpose of real-time traffic flow management.
69. The *Act* is not specific on minimum time limits necessary to deem that a collection has occurred. However, in the past, this Office has always interpreted the *Act*'s intended use of the verb "collect", within the context of collection of personal information, to describe an act of perceiving that information for any length of time, usually with a view to applying the information to a purpose. The fact that the organization chooses not to retain the information afterwards does not discount the reality of a collection having occurred in the first place.
70. Thus, I cannot accept Bell's assertion that there is no collection of the IP addresses linked to the subscriber user IDs. Since Bell has not implemented our fourth recommendation, Principle 4.8 is not upheld.



BELL'S OTHER COMMENTS

71. Bell also commented on this Office's usage of certain terms in our report of investigation, as well as a perceived lack of detail with which we occasionally expressed some of the facts. After carefully considering these comments, I am of the opinion that, in general, our report of investigation is an accurate account of our investigation, and in no way did the manner in which we choose to report on a complex and technical issue (to thereby include a more general readership) ultimately influence how we arrived at our recommendations or findings.
72. That being said, our description in paragraph 5 of how information is transmitted via the Internet could be clarified by removing the parenthesized phrase "or 'payload'" since, as Bell as has pointed out, one can consider there to be more than one payload where there are several consecutive protocol layers. In the final analysis, however, the notions of payloads and protocol layers were in no way central to our investigation's recommendations or findings.
73. Concerning the complainant's allegation of a broken web link between Bell's Terms of Service document and the Sympatico Privacy Policy (paragraphs 35-36), Bell contended that there still was confusion around this issue. In an effort to address the confusion, Bell offered the following:

... the complainant confused the terms that relate to the *Sympatico.MSN* portal www.sympatico.msn.ca, which is a multi-purpose portal that has nothing to do with Bell's Internet access services and the use of DPI technology, and the main Bell service website ww.bell.ca. ... In the *Sympatico.MSN Terms of Use*, however, it turned out that there was a broken link that has since been repaired. ... Furthermore, Bell explained that a prior version of the *Sympatico.MSN Terms of Use* continued to make reference to the Bell *Customer Privacy Policy* which was a simpler customer-focused document that used to accompany the Bell Code of Fair Information Practices. Bell confirmed that the Bell Customer Privacy Policy no longer exists and it was replaced by a one page Privacy Statement and a comprehensive list of FAQs on Bell's privacy pages that are updated as necessary. Bell also confirmed that the alleged broken link to the former Customer Privacy Policy had been repaired and that the content of the web page was updated.

Thus, the circumstances surrounding the once-broken web link have been explained.

74. Lastly, Bell provided further representations on the matter of whether customers, prior to the implementation of DPI technology, were advised that their traffic would be subject to inspection. According to the respondent, it posted a notice entitled "Network Management" on its website www.bell.ca on October 4, 2007,



before the roll-out of DPI began for its Sympatico customers in mid-October. According to Bell, the notice stated the following:

In order to continue to maintain a consistently high level of service for all of our customers, Bell may be required to manage its network in such a way that no customer, service or application consumes excessive bandwidth which may impede the use and enjoyment of other customers. This network management will allow Bell to deliver a consistent and reliable experience to all its customers who use real-time sensitive applications like browsing and instant messaging. Other providers here in Canada have implemented similar types of measures. It is important to note that all online applications will continue to be available to our valued customers.

This added information does not alter our investigation's recommendations or findings.

Conclusion

75. Accordingly, the complaint is not well-founded with regard to the two matters of consent and limiting collection, but well-founded with regard to the matter of openness.
76. We will be following up with Bell within 30 days to verify the status of the following:
 - the underlined heading to be added to the paragraph of the aforementioned service agreements (in clause 17 or 14) that pertains to the retaining or using of information from posted subscriber comments;
 - the answer to the privacy FAQ that will be added, relative to how Bell's traffic management practices impact the privacy of customers; and,
 - the suggested revisions to the answer to the question "What is Deep Packet Inspection (DPI) and what does it have to do with Internet traffic management?", found on Bell's "Network Management" web page, so as to indicate that personal information is collected.
77. Lastly, Bell confirmed in its report to the CRTC that it is not introducing any configurations of DPI as part of its traffic management solution that would allow the organization to inspect the content of user communications on its network. It also explained its stance on its transparency obligations when it chooses one particular technology over another: Citing its 310-BELL call-recording technology as an example, it has acknowledged that if this technology were used by Bell in



the future "... for a different purpose, e.g. marketing purposes, it would have to do so in compliance with the PIPEDA obligations, such that a new purpose would have to be identified, consent ... would have to be obtained prior to doing so and the form of consent would depend on the sensitivity of the information. No consent would be sought on the actual technology being used to do so."

78. Likewise, I would fully expect that, in accordance with Principle 4.4 of the *Act*, any expanded use of DPI by Bell in such a way that personal information is collected, used or disclosed for purposes other than the current purpose of managing network traffic, would require renewed, meaningful and informed consent from those individuals whose personal information would be affected. As well, pursuant to Principle 4.8, any resulting changes to the policies and practices of personal information management by the organization would have to be made readily available to individuals.