BEFORE THE CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION

IN THE MATTER OF AN APPLICATION BY THE PUBLIC INTEREST ADVOCACY CENTRE ("PIAC") AND THE CONSUMERS' ASSOCIATION OF CANADA ("CAC")
(APPLICANTS)

REGARDING BELL'S USE OF CUSTOMER INFORMATION

PURSUANT TO PART 1 OF THE *CRTC RULES OF PRACTICE AND PROCEDURE* AND SECTIONS 24, 32(g), 36, 47, 48, 55(c), and 56 of the *TELECOMMUNICATIONS ACT*

DIRECTED TO

BCE INC., BELL CANADA, BELL MOBILITY INC., AND BELL ALIANT REGIONAL COMMUNICATIONS, LIMITED PARTNERSHIP
(RESPONDENTS)

27 January 2014

Geoffrey White
Counsel for PIAC/CAC
(613) 562-4002 x24
gwhite@piac.ca

c/o Public Interest Advocacy Centre
One Nicholas Street, Suite 1204
Ottawa, Ontario K1N 7B7

TABLE OF CONTENTS

1. NATURE OF APPLICATION

1) The Public Interest Advocacy Centre ("**PIAC**"[1]) and the Consumers' Association of Canada ("**CAC**"[2], collectively "**PIAC/CAC**") file this Application with the Canadian Radio-television Telecommunications Commission (the "**Commission**" or the "**CRTC**") under Sections 24, 32(g), 36, 55(c), and 56 of the *Telecommunications Act*[3] (the "*Act*"), as well Part 1 and section 3 of the *CRTC Rules of Practice and Procedure*[4], regarding the practices of BCE Inc., Bell Canada, Bell Mobility Inc. ("**Bell Mobility**"), and Bell Aliant Regional Communications, Limited Partnership ("**Bell Aliant**"); and their affiliates[5] (collectively, "**Bell**" or the "**Respondents**"), in respect of Bell's use of customer information for behavioural marketing.

2) PIAC/CAC submit as part of this Application the following appendices:

- Appendix "A" – Bell's "Relevant Ads" Program Notice
- Appendix "B" – Research on Canadians' Attitudes toward Privacy
- Appendix "C" – Bell Privacy Policy

3) On or about October 18, Bell issued an "Important notice about how Bell uses information" (the "**Bell Notice**"). The Bell Notice, which is copied as Appendix "A" hereto, was delivered by email, and also made available online.

4) The Bell Notice described a new Bell marketing initiative involving customer profiling, online behavioural marketing, and personal information, including location-based data (the "**Bell Relevant Ads Program**"). The Bell Notice, and the program, appears to relate only to Bell Mobility subscribers, however Bell has indicated that it intends

1 PIAC is a non-profit organization that provides legal and research services on behalf of consumer interests, and, in particular, vulnerable consumer interests, concerning the provision of important public services. See Public Interest Advocacy Centre, online: http://www.piac.ca.

2 CAC is an independent, non-profit, volunteer-based charitable organization with a mandate to inform and educate consumers on marketplace issues, to advocate for consumers with government and industry, and work with government and industry to solve marketplace problems. See Consumers' Association of Canada, online: http://www.consumer.ca/index.php4

3 S.C. 1993, c. 38.

4 SOR/2010-277.

5 By virtue of Decision 2004-50 – *Follow-up to Telecom Decision CRTC 2002-76 – Location of the CSG and regulatory safeguards for affiliated carriers*, a Canadian carrier subject to common control with an ILEC will be required to comply with section 25 and other applicable provisions of the *Telecommunications Act* whenever the ILEC would be required to do so.

to expand the program to TV[6] and Internet customers "in the future."[7] It is unclear if the Bell Relevant Ads Program or any similar marketing initiative will be undertaken by or used in conjunction with any of Bell or Bell Aliant or Bell's Mobility's affiliates and direct and indirect subsidiaries including The Source (Bell) Electronics Inc., Bell ExpressVu, Limited Partnership, KMTS, NorthernTel, Limited Partnership, Télébec, Limited Partnership (Télébec) and Northwestel, or any mobile virtual network operators ("**MVNO**") which use the Bell Mobility network, including Virgin Mobile, Solo Mobile and PC Mobile.

5) Recipients and viewers of the Bell Notice were informed that, starting on 16 November 2013, "Bell will use certain information" about their "account and network usage for select purposes."[8] The Bell Notice provided illustrations of the categories of information (network usage information, account information) and the types of information (*e.g.*, browsing history, location, TV viewing, calling patterns, gender and age), that Bell would begin collecting. The Bell Notice also provided illustrations of how that information will be used. It appears from the language of the Bell Notice that the Bell Notice "supplements" the Bell Privacy Policy (see Figure 1 below).

6) For example, viewers of the Bell Notice were informed that Bell would be using the information to "create better business and marketing reports"; for "other companies to create business and marketing reports"; and to "make ads you see more relevant." [9]

7) The Bell Notice does not give full details of the information Bell indicated it would be collecting, nor full details about how information may be used and disclosed.

8) Furthermore, customers were not given the option to consent to that collection or use of information. Rather, customers were told "If you do not want us to use your information for any of the purposes described above, you can opt out." Effectively, subscribers were told that they had no choice when it came to receiving unfiltered and random advertisements: "You will receive unfiltered and random ads whether

---

6 Bell Canada operates at least two Class 1 regional broadcasting distribution undertakings (BDUs) serving various municipalities in Ontario and Québec. Bell Canada's licensing structure is depicted online at http://www.crtc.gc.ca/ownership/eng/cht143.pdf.

7 "Initially, Bell Mobility customers will be the first to benefit from this program but we look forward to expanding it to TV and Internet customers in the future."

("How does bell respect my privacy?" > "Customer usage and account information to design relevant marketing", online: http://support.bell.ca/Billing-and-Accounts/Security_and_privacy/How_does_Bell_respect_my_privacy?step=4).

8 Appendix "A", Bell Relevant Ads Program Notice.

9 Appendix "A", Bell Relevant Ads Program Notice.

you participate or not".[10] In *both* cases - the default "Relevant targeted ads" setting or the "Unfiltered random ads (opt-out)" setting - Bell tracks customer information and Bell customers receive advertisements.

9) Perhaps no other private organization in Canada has as much access to Information about Canadians as Bell.

10) PIAC/CAC contend in this application that the Bell Relevant Ads Program violates Canadians' reasonable expectation of privacy.

11) The Bell Relevant Ads Program has raised considerable public[11] and academic[12] concern.

12) Not only does Bell's opaque description of the Bell Relevant Ads Program raise many privacy issues relating to exactly what information Bell is collecting and how it is being used, it also brings into question whether Bell – a telecommunications

---

10 "How does bell respect my privacy?" > "Customer usage and account information to design relevant marketing", online: http://support.bell.ca/Billing-and-Accounts/Security_and_privacy/How_does_Bell_respect_my_privacy?step=4

11 See *e.g.*, OpenMedia.ca, "Canadians react to Bell's latest affront to citizens" (23 October 2013), online: https://openmedia.ca/blog/BellDataGrab

12 See *e.g.*: Michael Geist, "Is Bell's Plan to Monitor and Profile Canadians Legal?" (October 29, 2013), online: http://www.michaelgeist.ca/content/view/6984/135/

Michael Geist, "The Great Canadian Personal Data Grab Continues: Bell Expands Its Consumer Monitoring and Profiling" (21 October 2013) online: http://www.michaelgeist.ca/content/view/6977/125/

Paul Barter, "Let's Give Bell Canada the Backlash It Deserves", *The Huffington Post* (24 October 2013), online: http://www.huffingtonpost.ca/paul-barter/bell-privacy-flap_b_4158469.html

Christine Dobby, Bell's move to track customers' web history, TV viewing sparks probe by privacy regulator, *Financial Post* (22 October 2013), online: http://business.financialpost.com/2013/10/22/bells-move-to-track-customers-web-history-tv-viewing-sparks-probe-by-privacy-regulator/?__lsa=a22c-bdaa

> David Fewer, an intellectual property lawyer and director of the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa, said BCE's move raises questions about its neutral role as a service provider. "They're no longer acting as that big dumb pipe that's just focused on offering the best Internet service it can. Now it's focused on content," he said. "If privacy has any meaning at all, we have to start giving our consumers more control and demanding opt-ins to services that we may not need or want."

common carrier[13] and a private organization that may have an unmatched level of access to Information about Canadians - is overstepping its role of providing telecommunications services to the public for compensation by pursuing a business model that also includes using, and in some cases, disclosing, customer information for advertising and marketing services to the private sector for compensation.

13) That shift in character – from telecommunications common carrier to the public to also an advertiser - represents a fundamental challenge to the very nature of how telecommunications law expects carriers to operate.

14) The Senate of Canada, and an officer of Parliament, the Office of the Privacy Commissioner of Canada (the "**Privacy Commissioner**" or the "**OPC**"), have also taken steps to review Bell's program.

15) The Commission, however, is vested with unique authority. The Commission is charged with regulating and supervising the broadcasting and telecommunications systems in Canada.[14]

16) Crucially, the Commission has a statutory obligation to protect privacy. Canadian telecommunications policy has as one of its objectives "to contribute to the protection of the privacy of persons."[15]

17) In furtherance of that objective, the Commission has, for example, imposed customer confidentiality terms of service on all telecommunications service providers. Furthermore, in its various regulatory policies, including decisions to forbear from regulation, that Commission has retained its power under Section 24 of the *Telecommunications Act* to impose conditions of licence, and the authority to address privacy matters. The Commission has exercised that authority in such ways as through rules about Internet traffic management practices ("**ITMPs**")[16].

18) PIAC/CAC contend that aside from being contrary to the policy objectives, and to specific Commission rules about privacy, an overarching concern is that Bell's Relevant Ads program does not provide sufficient detail to customers about what

---

13 *Telecommunications Act*, Section 2(1).

14 *Canadian Radio-television and Telecommunications Commission Act*, R.S.C., 1985, c. C-22, Section 12; *Broadcasting Act* (S.C. 1991, c. 11), Section 5; *Telecommunications Act* (S.C. 1993, c. 38), Sections 7, 47, 48.

15 *Telecommunications Act*, section 7(i).

16 Telecom Regulatory Policy CRTC 2009-657 - *Review of the Internet traffic management practices of Internet service providers* (21 October 2009) (the "**ITMP framework**").

exactly Bell is collecting or how it will be used. Furthermore, a number of observers have raised concerns that the Bell Relevant Ads Program could set a dangerous precedent.[17]

19) As others have already pointed out, it is not clear what customers are actually opting out of when they choose to opt-out by selecting the "Unfiltered random ads" option.

20) The Commission's role is separate and distinct from Parliament and its Officers.

21) Indeed, the Privacy Commissioner has recognized the unique and important role that the CRTC has to play in protecting Canadians' privacy,[18] and has encouraged the Commission to take steps to address issues arising from online tracking, profiling and targeting.[19]

22) For the reasons which follow, PIAC/CAC contend that:

I). the Bell Relevant Ads Program is a violation of Canadians' reasonable expectations of privacy and is contrary to the *Telecommunications Act*, and, in particular, the policy objective of "the protection of the privacy of persons";

II). the Bell Relevant Ads Program is a violation of the Commission's ITMP framework and a violation of the privacy principle established in the ITMP framework;

III). the Bell Relevant Ads Program is a violation of the Commission's confidential customer information rules;

IV). the Bell Relevant Ads Program is a violation of Section 36 of the *Telecommunications Act*; and

V). the Bell Privacy Policy, which is oriented to PIPEDA, is insufficient to protect Canadians' privacy.

---

17 CBC News, "Privacy commissioner to investigate Bell's data collecting" (22 October 2013), online: http://www.cbc.ca/news/canada/montreal/privacy-commissioner-to-investigate-bell-s-data-collecting-1.2158593

18 Final reply of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) regarding Review of the Internet traffic management practices of Internet service providers (July 2009).

19 *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing* (May 2011).

23) PIAC/CAC therefore request that the Commission exercise its unique authority and recognized expertise and its statutory obligation to protect privacy by prohibiting Bell from collecting and using customer information for advertising and marketing purposes as set out in the Bell Relevant Ads Program.

24) In the alternative, PIAC/CAC request that the Commission direct Bell to make the Bell Relevant Ads program entirely opt-in; and to fully disclose all details of the collection, use and disclosure of the personal information to users in their privacy policies and related documents.

25) In both the primary and alternative relief scenarios, PIAC/CAC requests that the Commission order Bell to provide full details on the public record of the operation and nature of the Bell Relevant Ads Program, including the exact details of what information is being collected and how it is being collected, used and disclosed by Bell.

26) In making these requests PIAC/CAC highlight the Commission's findings that a higher standard of privacy protection than the basic standard under the *Personal Information Protection and Electronic Documents Act*[20] is necessary for customers of telecommunications services. PIAC/CAC also highlight the Privacy Commissioner's acknowledgement of that distinct possibility.

27) PIAC/CAC also request that the Commission initiate a larger, follow-up proceeding to examine the data collection and use practices of all other telecommunications service providers and BDUs.

2. FACTS

(a) Bell's Size, Scale and Access to Information about Canadians

28) Perhaps no other private organization in Canada has as much access to Information about Canadians as Bell.

29) Bell, through its various corporate and operating entities and affiliates, is a vertically integrated business acting in various regulated capacities including as a

[20] S.C. 2000, c. 5 ("**PIPEDA**").

telecommunications service provider (local and long distance wireline services; wireless, high-speed Internet); a broadcasting undertaking (radio, television and digital media services); and broadcasting distribution undertakings (satellite and IP television).[21]

30) As of the third quarter for 2013, Bell had:

- 7.8 million wireless subscribers;
- 5.3 million wireline telephony subscribers (business and residential);
- 2.2 million internet subscribers; and
- 2.2 million subscribers to its broadcasting distribution undertaking ("**BDU**") services (including Fibe TV and satellite).[22]

31) Bell telecommunications and broadcasting services play a role in many Canadians' lives, and may do so increasingly for those who buy Bell services in a bundle of two or more services. The more a customer uses Bell, the more information Bell could be in a position to exploit.

(b) Bell's "Four Screen" Strategy

32) Bell is on record as pursuing a "four-screen" strategy.

33) The four-screen strategy involves leveraging Bell's numerous media properties and distribution networks to increase "share of wallet" through more content and advertising being delivered to more television, smartphone, tablet and computer screens via an accompanying wireless, mobile Internet, TV and home Internet subscription.

34) In a 2011 interview on the Business News Network, Bell's President and Chief Executive Officer spoke about the four-screen strategy and Mr. Cope directly linked advertising opportunities to the four-screen strategy[23]:

> Mr. Cope: "We believe four screen viewing will be a tremendous opportunity for our shareholders going forward." (3:01)

21 See also Appendix "C" hereto, Bell Privacy Policy, "Scope and Application".

22 Bell, Third Quarter Financial Statements.

23 Business News Network, "Bell's Four-Screen Strategy", online: http://www.bnn.ca/News/2011/4/4/BCEs-Four-Screen-Strategy.aspx.

> Mr. Cope: "Moving the leadership position that the assets have had on what we would think as the traditional TV market and moving that onto the other three screens – we see that as a great opportunity." (3:00)

> Interviewer: "Correct my numbers if they're wrong here but online advertising about $100 million – TV advertising about $3 billion in this country. When do you see that flipping?
>
> Mr. Cope: "Oh I don't think we anticipate it flipping. I think what we see is opportunity for our customers viewing this content on these different screens, and from a shareholder perspective that drives subscription services." (3:30)

35) Advertising revenue appears to be a major strategy focus of Bell Media – the content-providing side of Bell's business. Bell has acknowledged for Bell Media has a "significant dependence on a continued demand for advertising"[24], and in numerous disclosures has noted plans to drive advertising revenue. For example:

> We anticipate a stable advertising market in 2013 and expect to drive advertising revenue growth through improved market share. Growth in subscriber revenues is expected to come from contracted rate increases for our specialty sports services. **Our plan is to continue to invest in premium content for all four screens,** while carefully managing costs by leveraging assets, achieving productivity gains and pursuing operational efficiencies. In 2013, we intend to launch our TV Everywhere product, which is a strategic initiative that will enable us to deliver the best live sports, news and other premium content exclusively to broadcasting distribution undertakings (BDUs) subscribers.
>
> In conventional TV, **we intend to leverage the strength of our market position to continue offering advertisers, both nationally and locally, with premium opportunities to reach their target audiences.** Success in this area requires that we focus on a number of factors, including building and maintaining strategic supply arrangements for content on four screens, continuing to successfully acquire high-rated programming and differentiated content to execute on Bell's multi-screen content strategy, producing and commissioning high-quality Canadian content, as well as producing market-leading news through investments in HD broadcasting and improvements to our news programming.[25]

36) Bell is clearly committed to a path of increasing advertising revenue via its four-screen strategy, and the Bell Relevant Ads Program appears to be a first step on that path.

---

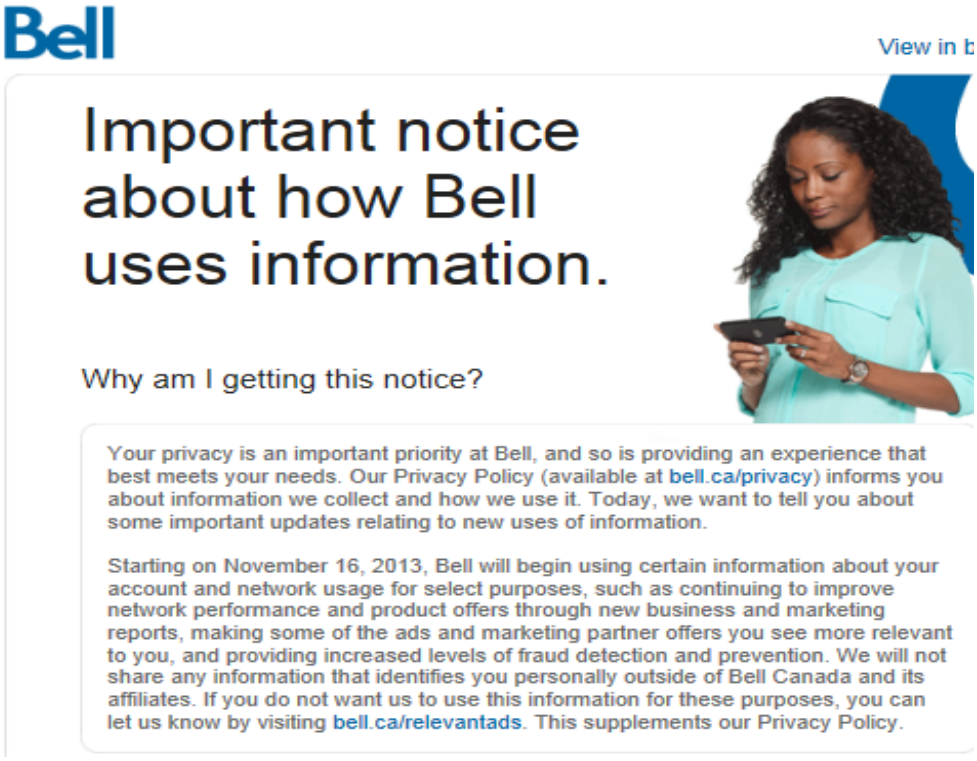
[24] BCE Inc. press release, BCE reports first quarter 2013 results (9 May 2013), online: http://www.bce.ca/news-and-media/releases/show/bce-reports-first-quarter-2013-results.

[25] Bell's Business Outlook and Assumptions (part of Management Discussion in Annual Report 2012), online, http://www.bce.ca/annual-reports/2012-annual-report/managements-discussion-and-analysis/business-outlook-and-assumptions/ (emphasis added).

(c) The Bell Relevant Ads Program

37) On or about October 18, 2013, less than one month prior to the start of the Bell Relevant Ads Program, Bell issued an "Important notice about how Bell uses information" (the "**Bell Notice**"). The Bell Notice, which is copied as Appendix "A" hereto, was delivered by email, and also made available online. The introduction to the announcement is excerpted in Figure 1 below.

Figure 1 – Bell's Notice

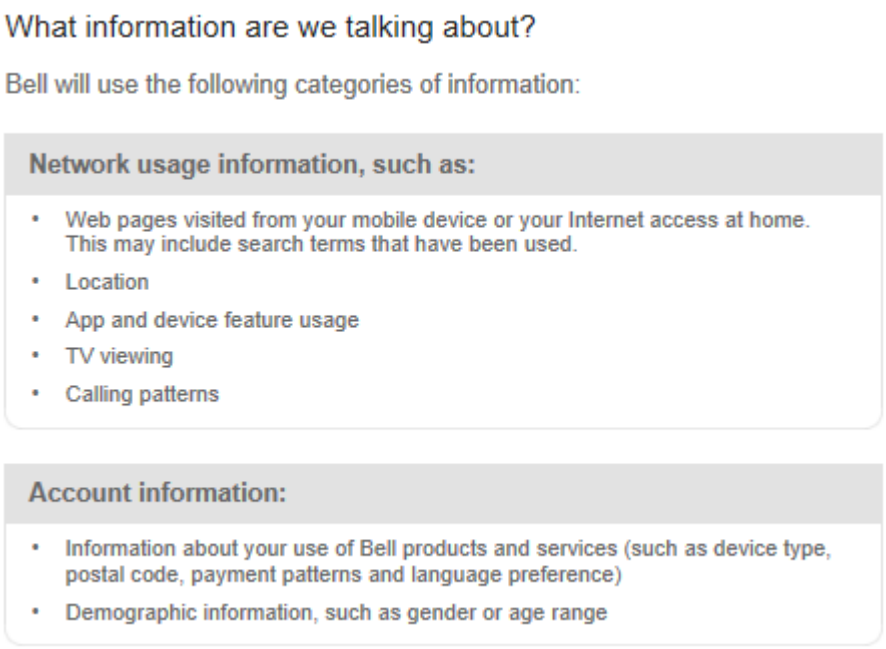


38) The Bell Notice described a new Bell marketing initiative involving customer profiling, online behavioural marketing, and personal information, including location-based data (the "**Bell Relevant Ads Program**"). The Bell Notice, and the Bell Relevant Ads Program, appears to relate only to Bell Mobility subscribers.[26]

[26] "Initially, Bell Mobility customers will be the first to benefit from this program but we look forward to expanding it to TV and Internet customers in the future." ("How does bell respect my privacy?" > "Customer usage and account information to design relevant marketing", online: http://support.bell.ca/Billing-and-Accounts/Security_and_privacy/How_does_Bell_respect_my_privacy?step=4)

39) Recipients and viewers of the Bell Notice were told that, starting on 16 November 2013, "Bell will use certain information" about their "account and network usage for select purposes."[27] The notice provided illustrations of the categories of information (network usage information, account information) and the types of information (*e.g.*, browsing history, location, TV viewing, calling patterns, gender and age), that Bell would begin collecting. An excerpt of the Bell Notice is provided at Figure 2 below.

Figure 2 – Illustrative List of Data Being Collected by Bell



40) The Bell Notice provided a general description of what customers' information might be used for, and it also provided illustrations of how that information will be used.

41) For example, the Bell Notice explained that Bell would be using the information to "create better business and marketing reports"; for "other companies to create business and marketing reports"; and to "make ads you see more relevant."[28] It is not clear from the Bell Notice exactly what information will be collected and used by Bell or other parties, or how it will be used. The information provided by Bell is illustrative at best, and does not give a complete explanation of exactly what data is being collected, how it will be used, nor how it will be disclosed.

27 Appendix "A", Bell Relevant Ads Program Notice.

28 Appendix "A", Bell Relevant Ads Program Notice.

42) Aside from not being given sufficient, specific information about exactly what information will be collected by Bell and other parties, or how it will be used, or how it will be disclosed, customers were not given the option to consent to that collection of information. Rather, they were told "If you do not want us to use your information for any of the purposes described above, you can opt out." Furthermore, subscribers were told that they had no choice when it came to receiving unfiltered and random ads. "You will receive unfiltered and random ads whether you participate or not".[29]

43) In other words, Bell does not give subscribers any meaningful choice over their privacy. In *both* cases - the default "Relevant targeted ads" setting or the "Unfiltered random ads (opt-out)" settings, Bell nevertheless tracks customer information and Bell customers receive advertisements. Presumably, in the "Unfiltered random ads (opt-out)" scenario, Bell nevertheless uses and discloses aggregated customer information for marketing purposes.

44) The Bell notice raised considerable concerns from the public and from academics about privacy.[30] Furthermore, on October 23, 2013, the Privacy Commissioner of Canada (the "**Privacy Commissioner**") announced it would be investigating the

---

[29] "How does bell respect my privacy?" > "Customer usage and account information to design relevant marketing", online: http://support.bell.ca/Billing-and-Accounts/Security_and_privacy/How_does_Bell_respect_my_privacy?step=4

[30] See *e.g.*:

OpenMedia.ca, "Canadians react to Bell's latest affront to citizens" (23 October 2013), online: https://openmedia.ca/blog/BellDataGrab

Michael Geist, The Great Canadian Personal Data Grab Continues: Bell Expands Its Consumer Monitoring and Profiling (21 October 2013), online: http://www.michaelgeist.ca/content/view/6977/125/

Paul Barter, "Let's Give Bell Canada the Backlash It Deserves", *The Huffington Post* (24 October 2013), online: http://www.huffingtonpost.ca/paul-barter/bell-privacy-flap_b_4158469.html

Christine Dobby, Bell's move to track customers' web history, TV viewing sparks probe by privacy regulator, *Financial Post* (22 October 2013), online: http://business.financialpost.com/2013/10/22/bells-move-to-track-customers-web-history-tv-viewing-sparks-probe-by-privacy-regulator/?__lsa=a22c-bdaa

> David Fewer, an intellectual property lawyer and director of the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa, said BCE's move raises questions about its neutral role as a service provider. "They're no longer acting as that big dumb pipe that's just focused on offering the best Internet service it can. Now it's focused on content," he said. "If privacy has any meaning at all, we have to start giving our consumers more control and demanding opt-ins to services that we may not need or want."

CBC News, "Bell data collection part of 'disturbing trend'", online: http://www.cbc.ca/news/technology/bell-data-collection-part-of-disturbing-trend-1.2223949

notice.[31] On 4 December 2013 notice of motion was given in the Senate of Canada to hear from representatives of Bell and the Privacy Commissioner about the Bell Relevant Ads Program.[32]

(d) Technology continues to threaten privacy

45) The well-documented rise in the use of technology and constant connectivity to the Internet and use of the Internet (both wireline and wireless access) to deliver telecommunications and broadcasting services can pose serious threats to privacy.

46) More than a decade ago - in an update to the confidentiality obligations imposed on Canadian carriers to protect the confidentiality of customer information - the Commission noted that those obligations "are even more relevant today than when they were first implemented, due to the advent of new technologies and the emergence of electronic commerce, which allow information to be easily processed, re-arranged and exchanged."[33]

47) That was in 2003 – on the doorstep of so many new technologies and services through which many Canadians now experience their lives.

48) In 2009 the Commission again noted that "protecting the privacy of telecommunications service customers was increasingly important due to the advent

---

31 Announcement, **October 23, 2013, "**Privacy Commissioner to investigate Bell Canada's privacy policy changes**"** Online: http://www.priv.gc.ca/media/nr-c/2013/an_131023_e.asp

32 Hon. Leo Housakos: Notice of Motion to Authorize Committee to Hear Witnesses from BCE Inc. (Bell Canada) and the Privacy Commissioner Regarding Use of Customer Data.

Honourable senators, I give notice that, at the next sitting of the Senate, I will move:

> That the Standing Senate Committee on Transport and Communications be authorized to hear from representatives from BCE Inc. (Bell Canada) and the Privacy Commissioner of Canada regarding the practice of collecting and analyzing data from Bell Canada customers for commercial purposes including targeted advertising[.]

Note: On 9 December 2013 the motion for study was put before the Senate. Limited debate on the motion revealed the study would involve 2 meetings: 1) Privacy Commissioner, 2) Bell. The meetings will be in Ottawa. The Senate adopted the motion so that the Senate Transportation and Communications committee can undertake its study. As of the time of this Application the Senate has not resumed sitting.

33 Telecom Decision CRTC 2003-33 - *Confidentiality provisions of Canadian carriers* (30 May 2003), as amended by Telecom Decision CRTC 2003-33-1, at para. 24.

of new technologies and the emergence of electronic commerce, which enable information to be more easily processed, rearranged, and exchanged."[34]

49) In the words of the Privacy Commissioner, "As information technologies become more and more common in our lives, and the more they become an extension of our very selves, the more sensitive and revealing subscriber identification information becomes."[35]

50) The Government of Canada flagged the seriousness of the issue in its 2010 consultation on a Digital Economy for Canada.

> Some emerging technologies and online applications raise new questions about the protection of personal information. Current concerns include third party use of personal information mined by search engine operators and collected through social networking sites, as well as the personal tracking capabilities of geo-location technologies. New privacy and security challenges are also posed by the development of web-based services and cloud computing (which replace dedicated ICT equipment and software under the direct control of individual consumers and business users with shared facilities managed by third party service providers). The Government of Canada tracks emerging issues and participates in domestic and international fora to ensure its policy and legislative regimes are up-to-date and promote the growth of the online marketplace.[36]

51) PIAC/CAC have also raised privacy concerns on a number of occasions, including:

- A 2008 report titled "All in the Data Family: Children's Privacy Online"[37], reviewing the privacy risks to children when commercial entities target children through personal information collected when children join online playgrounds;
- A 2009 report titled "A 'Do Not Track List' for Canada"[38], examining online behavioural targeted advertising and online behavioural tracking.
- A 2009 complaint to the Privacy Commissioner of Canada under the *Personal Information Protection and Electronic Documents Act* regarding Nexopia's

---

34 Telecom Regulatory Policy CRTC 2009-657 - *Review of the Internet traffic management practices of Internet service providers* (21 October 2009) at para. 101.

35 Office of the Privacy Commissioner of Canada, *What an IP Address Can Reveal About You* (May 2013) at 9.

36 *Improving Canada's Digital Advantage - Strategies for Sustainable Prosperity* - Consultation Paper on a Digital Economy Strategy for Canada (May 2010).

37 Public Interest Advocacy Centre, "All in the Data Family: Children's Privacy Online" (September 2008).

38 Public Interest Advocacy Centre, "A 'Do Not Track List' for Canada?" (December 2009).

privacy practices and the particular vulnerability of youth using social networking services.[39]

- Submissions to the Commission in its review[40] of ITMPs.

- Testimony before the House of Commons, Standing Committee on Access to Information, Privacy and Ethics ("**ETHI**") as part of its study on the efforts and the measures taken by social media companies to protect the personal information of Canadians.[41]

52) The scale and scope of the business opportunities associated with the amount of data about consumers available through the use of technology is said to be unprecedented, particularly given the rise in the use of location-based technologies that add a customer's whereabouts to the mix of information potentially available about a given person.

53) As the Privacy Commissioner's research indicates:

> "The types of information collected in log files about Internet users can include: Internet Protocol (IP) address; pages visited (on a single site or across sites); length of time spent on pages; advertisements viewed; articles read; purchases made; search terms or other information entered on a site; user preferences such as language and web browser type; operating system; and geographical location information, through IP addresses (on the web) or the Global Positioning Systems (GPS) common in many mobile communications devices."[42]

54) In addition:

> [K]nowledge of subscriber information, such as phone numbers and IP addresses, can provide a starting point to compile a picture of an individual's online activities, including:
>
> - Online services for which an individual has registered;
> - Personal interests, based on websites visited; and
> - Organizational affiliations.
> - It can also provide a sense of where the individual has been physically […][43]

---

39 18 January 2009.

40 Telecom Public Notice CRTC 2008-19 – *Review of the Internet traffic management practice of Internet service providers* (20 November 2008).

41 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1550 (John Lawford, PIAC).

42 Privacy Commissioner of Canada, "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing" (May 2011) online: https://www.priv.gc.ca/resource/consultations/report_201105_e.asp

43 Office of the Privacy Commissioner of Canada, *What an IP Address Can Reveal About You* (May 2013) at 9.

55) In PIAC's submission in 2010 to the Government of Canada in its Consultation on a Digital Economy for Canada, PIAC underscored the seriousness of this concern.

> Since the introduction of the world wide web, rapid changes introducing digital technologies only seem to be picking up speed and changing consumer expectations. With the introduction of smartphones and their increasing popularity, we are moving towards the societal expectation of ubiquitous internet access from all electronic devices. This rapid shift heightens privacy and security concerns as consumers use these devices to participate in electronic commerce and constant social connectivity through social networking services. Governments have struggled to keep pace as innovative digital technologies and new business models evolve quickly and antiquated laws that were designed to protect tangible property and apply to analog networks and legacy systems no longer seem applicable or seemingly produce unreasonable results.[44]

56) In 2014 these predictions have certainly been borne out, and the Internet is the medium through which Canadians experience much of their personal and professional lives and IP connectivity[45] is becoming the medium of choice for delivery of telecommunications services and broadcasting. As the record of the Commission's ITMP framework proceeding indicates, as do submissions to the Privacy Commissioner's Deep Packet Inspection Essay Project[46], deep packet inspection ("**DPI**") technology can also be used to go far beyond merely transmitting data, but to actually peer within the data itself.

57) In a 2009 research report, PIAC predicted that as mobile technology pushed ahead, location-specific behaviourally targeted marketing on mobile devices would be the next logical step for marketers.[47]

58) As the business literature notes, the scale and scope of the opportunities that will be enabled by location-based technologies are unprecedented. According to one consultancy, "Digital and mobile delivery platforms enable brands to deliver messages and engage with their consumers *at a level of intimacy never achievable*

---

44 Public Interest Advocacy Centre, Submission to the Government Consultation on A Digital Economy Strategy for Canada (14 July 2010) at 6.

45 The Commission has recognized the move towards IP-connectivity. For example: "In the Commission's view, the transition to IP-based networks is imperative to the creation of a digital economy that will benefit all Canadians by fostering opportunities for innovation in new services." Telecom Regulatory Policy CRTC 2012-24 – *Network interconnection for voice services* (19 January 2012) at para. 23. Also, Commissioner Timothy Denton noted the move to an "all-Internet protocol communications system" in *A Report on Matters Related to Emergency 9-1-1 Services* (dated 5 July 2013, publically released 10 October 2013), as para. 24.

46 Online: http://www.priv.gc.ca/information/research-recherche/dpi_index_e.asp.

47 Janet Lo, The Public Interest Advocacy Centre, "A Do Not Track List for Canada" (October, 2009) online: http://www.piac.ca/files/dntl_final_website.pdf.

before. … LBM [location-based marketing] offers the ability to understand customer profiles, behaviours, and purchasing habits *well beyond traditional measurement* of marketing and advertising spending. And *we are not just talking about smartphones and tablets*."[48]

59) With the rapid growth in adoption and use by Canadians of smartphones with embedded GPS chips, and by business of Radio Frequency Identification (RFID) technology, and location-based data being a part of an increasing number of applications in use, the opportunities for businesses to gain even more insights into consumer behaviour based on consumers' whereabouts are said to be unprecedented.

60) At an October 2013 workshop on online advertising, the President of the Location-Based Marketing Association, an industry association, noted that 85 per cent of data has a location element to it, and that "Location is the new cookie".[49]

61) Bell, as one of Canada's largest telecommunications and broadcasting companies and major providers of the connectivity appears to now be seeking to capitalize on all the information its primary role is to transmit as a telecommunications service provider.

(e) Canadians are concerned about privacy, generally

62) Privacy is a fundamental value for Canadians. In addition to having expression in the *Canadian Charter of Rights and Freedoms*[50], it is also one of the objectives of Canadian telecommunications policy.

---

48 PriceWaterhouseCoopers "Marketing goes local: Location-based marketing provides solutions to technology's disruption of product promotion, placement and pricing." Online: http://www.pwc.com/en_CA/ca/entertainment-media/publications/pwc-marketing-goes-local-2012-08-20-en.pdf (emphasis added) (May 2012).

49 Online Advertising in Canada: Workshop on Emerging Business, Consumer & Regulatory Issues, (October 1, 2013), online: http://onlineadvertisingworkshop.ca/2013/

50 See *R. v. TELUS Communications Co*., 2013 SCC 16; see also *Privacy Commissioner, et al. v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, at para. 19:

> The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society[.]

63) Unsurprisingly, therefore, Canadians are concerned about privacy, and especially so in the online environment.

64) This is evidenced by such initiatives as OpenMedia.ca's "Protect our Privacy" grassroots campaign, or the widespread concerns about the Government of Canada's attempt to update the legislation for lawful interception.[51]

65) This is part of a broader concern about the privacy implications of new technologies.

66) A majority of Canadians, according to an April 2013 study released by the Privacy Commissioner of Canada, have difficulty understanding how new technologies affect their privacy.[52] The number of Canadians lacking confidence in their ability to protect their privacy in the face of new technology has increased steadily since the year 2000.[53] As a result, it is no surprise 55% reported being very concerned about posting information about their location, and seven in ten Canadians feel they have less protection of their personal information in their daily lives than they did 10 years ago.[54] This sentiment is seemingly summed up in a quote from Lee Tien of the Electronic Frontier Foundation when he noted, prior to the Internet, "you were private by default and public by effort. Nowadays, you are public by default and private by effort."[55]

67) Previous research, conducted in the context of group buying programs and loyalty problems, illustrate the concerns Canadians have with privacy.

---

51 See *e.g.*,CBC News, "Government killing online surveillance bill", February 11, 2013 online: http://www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384

52 Privacy Commissioner of Canada, *Canadians increasingly anxious about privacy in the face of new technology, poll suggests*, News Release, April 4, 2013. Last accessed April 18, 2013 at http://www.newswire.ca/en/story/1140765/canadians-increasingly-anxious-about-privacy-in-the-face-of-new-technology-poll-suggests

53 Privacy Commissioner of Canada, *Canadians increasingly anxious about privacy in the face of new technology, poll suggests*, News Release, April 4, 2013. Last accessed April 18, 2013 at http://www.newswire.ca/en/story/1140765/canadians-increasingly-anxious-about-privacy-in-the-face-of-new-technology-poll-suggests

54 Privacy Commissioner of Canada, *Canadians increasingly anxious about privacy in the face of new technology, poll suggests*, News Release, April 4, 2013. Last accessed April 18, 2013 at http://www.newswire.ca/en/story/1140765/canadians-increasingly-anxious-about-privacy-in-the-face-of-new-technology-poll-suggests

55 Pearson, Bryan, *The Loyalty Leap: Turning Customer Information into Customer Intimacy*, Penguin Group, Toronto, 2012, P. 39. From Joel Stein, "Data Mining: How Companies Now Know Everything About You," *Time*, March 10, 2011.

68) In 2005, Union des consommateurs noted that previous survey data commissioned by PIAC suggested 82% of respondents said that companies should obtain their permission before using their information for marketing purposes, that 69% of respondents found current "withdrawal of consent" business practices totally unacceptable and they preferred that companies explicitly request customer consent when they wanted to use customer personal information for marketing purposes.[56] Since that time, an argument can be made that Canadians still value their privacy despite rhetoric that privacy is less regarded in the social media age.

69) In previous research on loyalty programs PIAC noted that Canadian consumers want to know what data is being collected about them, as well as to provide their permission before being tracked online or by physical location.**[57]** It is reasonable to believe that Canadian consumers would hold similar, if not more strident views, in respect of information being collected by their telecommunications service provider, who, in the case of vertically-integrated companies, may also be their one source for all communications services including home phone, home Internet, wireless phone and mobile Internet, broadcasting distributor, and programming provider.

70) In other research conducted on behalf of PIAC, it was observed that consumers were not comfortable with unfettered collection and use of their personal information overall. Specifically, when asked about their comfort level with online tracking for the purpose of targeted and behavioural advertising, only 8% of respondents responded that they were "very comfortable" and 17% were "somewhat comfortable". By contrast, a full 25% were "not very comfortable" and nearly half (49%) indicated they were "not at all comfortable" with such tracking. An even higher percentage of respondents expressed discomfort with companies and organizations that share information about their behaviours as consumers with third party organizations for the purpose of targeting advertising, with 25% "not very comfortable" and 53% "not at all comfortable".

(f) Canadians are specifically concerned with the Bell Relevant Ads Program

71) Canadians are specifically concerned about the Bell Relevant Ads Program.

---

56 Union des consommateurs, *Marketing de fidélisation: Qui récolte la meilleure récompense?*, (July 2005) at 15-16, from Les Associés de Recherche Ekos Inc. 2001. Utilisation professionnelle des renseignements personnels des consommateurs : ce qu'en pense le public. Préparé pour : Le Centre pour la défense de l'intérêt public (August 2001), online: <http ://www.ekos.ca>, at 42.

72) The investigative actions by the Privacy Commissioner[58] and the Senate[59] are also indicative of that concern.

73) So too is research cited by the Privacy Commissioner, excerpted in Appendix "B". That research suggests that at least half of Canadians are concerned with the use of their information for the purposes of targeting ads. The 2011 KPMG finding that only "46% of Canadians were 'somewhat willing' to have their online usage[60] tracked by advertisers, particularly when that tracking provided a "payoff" (*i.e.*, free service).[61]

74) That suggests that most Canadians are unwilling to have their online usage tracked, and, importantly, that those who may be willing to have their online usage tracked may view some form of a trade-off between the tracking and use of their information, and free services, as the ad-supported model of other free services, for example, may illustrate.

75) Customers of Bell are, however, paying Bell to provide telecommunications services and to transport their information. With Bell now also entering the business of profiting off of customer information, Bell appears to be "double-dipping" by taking both subscription fees for telecommunications services, and advertising opportunities and revenue based on customer information. No longer is Bell solely providing telecommunications services to the public for compensation, as the *Telecommunications Act* contemplates, but now Bell also appears to be in the business of advertising and advertising services.

76) These concerns come to life in public comments made about the Bell Relevant Ads Program. For example, the following comments on the popular social media site Reddit[62] illustrate some of the concerns being expressed.

58 *Supra*, note 29.

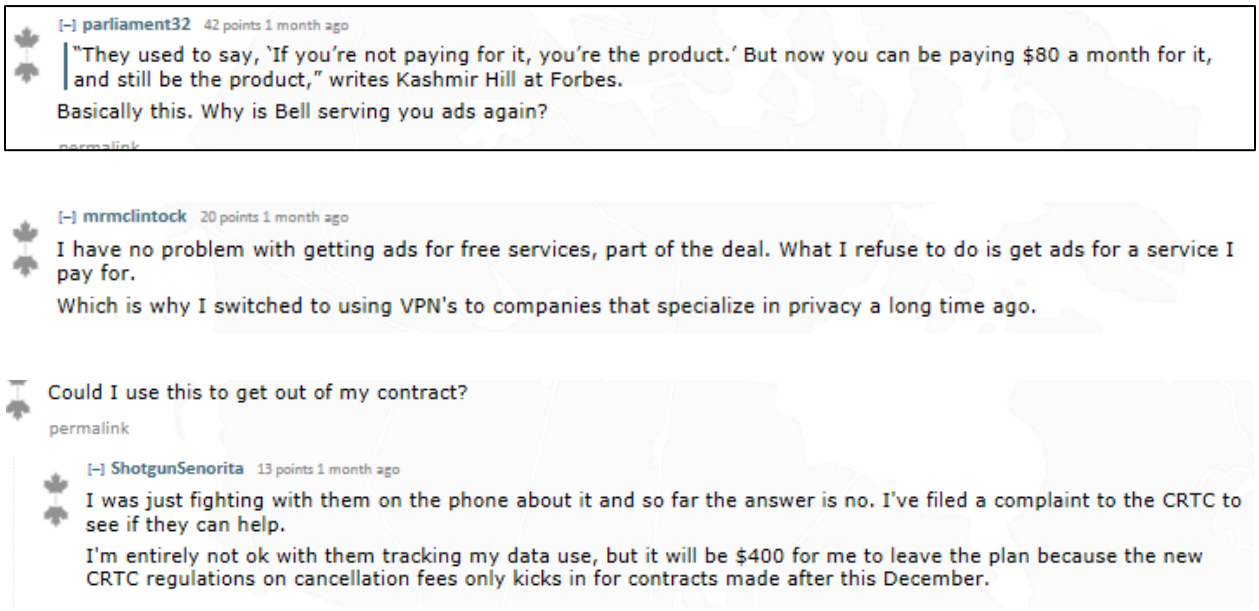
59 *Supra*, note 30.

60 Note, this does not explicitly include location-based data.

61 See Appendix "B" – Research on Canadians' Attitudes toward Privacy.

62 Online: http://www.reddit.com/r/canada/comments/1oz2wm/bell_canada_to_track_web_tv_surfing_habits_for_ad/

Figure 3
Select Public Concerns with
Bell Tracking / Profiting from Customer Information



77) Canadians are *clearly concerned* about their telecommunications service providers being in the business of not just transmitting communications, but tracking those communications and profiting off their personal usage profiles and characteristics. That concerns highlights the *conflict of interest* a telecommunications service provider is in when it expands its role of providing telecommunications services to the public for compensation by pursuing a business model that also includes providing customer information for advertising and marketing services to the private sector for compensation. That tension brings to the fore specific safeguards in the *Telecommunications Act* and in Commission policy against improper uses of customer information.

3. GROUNDS OF APPLICATION

78) PIAC/CAC contend that:

I). the Bell Relevant Ads Program is a violation of Canadians' reasonable expectations of privacy and is contrary to the *Telecommunications Act*, and, in particular, the policy objective of "the protection of the privacy of persons";

II). the Bell Relevant Ads Program is a violation of the Commission's ITMP framework and a violation of the privacy principle established in the ITMP framework;

III). the Bell Relevant Ads Program is a violation of the Commission's confidential customer information rules;

IV). the Bell Relevant Ads Program is a violation of Section 36 of the *Telecommunications Act*; and

V). the Bell Privacy Policy, which is oriented to PIPEDA, is insufficient to protect Canadians' privacy.

(I) The Bell Relevant Ads program is a violation of Canadians' reasonable expectations of privacy and is contrary to the *Telecommunications Act* and, in particular, the policy objective of "the protection of the privacy of persons"

79) The Commission is required to exercise its powers and perform its duties under the *Telecommunications Act* with a view to implementing the Canadian telecommunications policy objectives in Section 7.[63]

80) The Canadian telecommunications policy objectives include a number of social goals, and, explicitly, the protection of privacy. Specifically, Section 7 states:

> 7. It is hereby affirmed that telecommunications performs an essential role in the maintenance of Canada's identity and sovereignty and that the Canadian telecommunications policy has as its objectives:
>
> (a) to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions…;
>
> (h) to respond to the economic and social requirements of users of telecommunications services; and
>
> [...]
>
> (i) to contribute to the protection of the privacy of persons.

81) The Commission has, in furtherance of the telecommunications policy objective of the "protection of the privacy of persons" in Section 7(i) of the *Telecommunications*

[63] *Telecommunications Act*, Section 47.

Act, imposed confidentiality obligations on Canadian carriers in respect of both tariffed and forborne telecommunications services (except forborne mobile wireless services that are not switched, such as paging).[64]

82) In light of the concerns about the Bell Relevant Ads program cited above, and about compliance with specific Commission rules and policies cited below, the Bell Relevant Ads Program appears to be inconsistent with the telecommunications policy objective of contributing to "the protection of the privacy of persons".

83) As explained in Section 2(a), perhaps no other private organization in Canada has as much access to information about Canadians as Bell.

84) Bell may have an unmatched level of access to Information about Canadians by virtue of its size and scale as a telecommunications service provider, broadcaster and BDU.

85) With Bell now tracking web pages visited, location, application and device feature usage, TV viewing, calling patterns, information about the use of Bell products, gender and age range[65], it is not difficult to imagine the scale and scope of the privacy risks to Canadians, and the scale and scope of the advertising opportunities and revenue Bell may be tempted to solicit from its traditional business of providing telecommunications services to the public.

86) The Bell Relevant Ads Program, in leveraging Bell's size and scale to collect and use information about customers, therefore represents an unprecedented collection, use and disclosure by a telecommunications service provider of information about Canadians.

87) As explained in Sections 2(b) and 2(c) above, Canadians have a reasonable expectation of privacy, a point underscored by the research cited by the Privacy Commissioner and excerpted as Appendix "B".

88) The Bell Relevant Ads Program, which appears to be part of a broader four-screen strategy that emphasizes advertising revenue, is therefore a violation of that expectation.

---

64 See Telecom Decision CRTC 2003-33 - *Confidentiality provisions of Canadian carriers* (30 May 2003), as amended by Telecom Decision CRTC 2003-33-1, at para. 1.

65 Bell Relevant Ads Program Notice.

(II) The Bell Relevant Ads Program is a violation of the Commission's ITMP framework and a violation of the privacy principle reflected in the ITMP framework.

89) PIAC/CAC contend that the Bell Relevant Ads Program violates the Commission's rules for ITMPs, as set out in Telecom Regulatory Policy CRTC 2009-657[66] (the "**ITMP framework**").

90) The ITMP framework applies to both wireline and wireless Internet access.[67] The framework expressly prohibits, by way of a condition of providing service, the use and disclosure by ISPs of personal information collected for the purposes of traffic management.

> 100. The Commission notes that the privacy concerns raised on the record are founded on the potential uses of technologies employed by ISPs to implement ITMPs, rather than their current uses. The Commission also notes, however, that certain technologies have the capacity to collect and use personal information as part of an ITMP and that information obtained in this manner can be derived from the flow of network traffic, without the knowledge or consent of the consumer. For these reasons, the Commission considers that certain ITMPs raise privacy concerns in regard to the collection and use of personal information.
>
> 103. In light of the above, the Commission finds it appropriate to establish privacy provisions in order to protect personal information. The Commission therefore directs all primary ISPs, as a condition of providing retail Internet services, not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information. [68]

91) PIAC/CAC contend that in using customers' "network usage information, such as: web pages visited from your mobile device or your Internet access at home" and "App and device feature usage" [69] – *i.e.*, information about customers' use of networks for purposes other than traffic management, Bell Relevant Ads Program is a violation of the ITMP framework's prohibition against the collection and use of

---

66 Telecom Regulatory Policy CRTC 2009-657 - *Review of the Internet traffic management practices of Internet service providers* (21 October 2009).

67 Telecom Decision CRTC 2010-445 - *Modifications to forbearance framework for mobile wireless data services* (30 June 2010) at para. 11.

68 Telecom Regulatory Policy CRTC 2009-657 - *Review of the Internet traffic management practices of Internet service providers* (21 October 2009) at para. 103.

69 Appendix "A", Bell Relevant Ads Program Notice.

personal information as part of an ITMP or via the flow of network traffic or through DPI technology .

92) Moreover, the Bell Relevant Ads Program appears to contradict what Bell said in the proceeding on the ITMP framework about its own use of ITMPs.

93) In arguing against special privacy protections governing the use of ITMPs, Bell suggested it could not and would not use network information for marketing purposes:

> The Companies can confirm that the DPI [deep packet inspection] technology deployed in our networks is being deployed only for purposes of traffic management. Our DPI does not, and cannot, inspect the user content of communications. Data collected is used at an aggregate level to better understand the nature of traffic on our network and identify trends such as increases in the use of particular applications. It is not being used for marketing purposes.[70]

> First, the Companies stated that "[a]lthough the Companies DPI equipment does not, and cannot, inspect the user content of communications, all ISPs have the *capability* of inspecting the content of user communications.[71]

94) Bell claimed it did not have (at that time) the willingness or capacity to use DPI to inspect the content of communication, but also stated all ISPs could have that capability. Thus, at the time of the policy review and in arguing against more stringent privacy protections than provided for under PIPEDA, Bell said it was not using DPI information for "marketing purposes" and implied that it would not be doing so.[72] If that remains true, then Bell is clearly with the Bell Relevant Ads Program using customer information generated through the use of its networks and various services (home phone, wireless, Internet) for marketing in a manner contrary to the intent of the ITMP framework and to the position that Bell took in that proceeding.

95) PIAC/CAC also note Bell's statement, in the same submission, that "Personal information collected for the purposes of ITMPs should not be used for any other purpose without customer consent."[73] Bell there recognizes that explicit customer consent should be required in order to use personal information – collected for the purposes of ITMPs - for the purposes of marketing and advertising, as in the case of

---

70 *Supra* note 16 at para. 26.

71 *Ibid.*, at para. 27 (emphasis original).

72 *Ibid*.

73 *Ibid.* at para. 10.

the Bell Relevant Ads Program. Bell does not, however, seek explicit, informed customer consent for the Bell Relevant Ads Program, rather, it only gives customers the opportunity to opt out of Bell's behavioural marketing program, and not the opportunity to opt out of being tracked and targeted in the first place. In other words, Bell is relying upon implicit consent.

96) In the event that the Commission finds the Bell Relevant Ads Program technically does not make use of information collected as part of an ITMP for the purposes of traffic management or through the flow of network traffic or through DPI technology, and in the alternative to the PIAC/CAC contention that the Bell Relevant Ads Program is a violation of the ITMP framework, PIAC/CAC argues that the ITMP framework reflects a broader privacy principle and that the Bell Relevant Ads Program is a violation of that principle.

97) The Commission imposed the prohibition against the use and disclosure of personal information collected for the purposes of traffic management after having concluded that:

- certain ITMPs raised privacy concerns in regard to the collection and use of personal information;

- protecting the privacy of telecommunications service customers was increasingly important due to the advent of new technologies and the emergence of electronic commerce, which enable information to be more easily processed, rearranged, and exchanged;

- the Commission's role in protecting privacy was, given Section 7(i) of the *Telecommunications Act*, "complementary" to that of the Privacy Commissioner; and

- a "higher degree of privacy protection for customers of telecommunications services" was appropriate.[74]

[74] Telecom Regulatory Policy CRTC 2009-657 - *Review of the Internet traffic management practices of Internet service providers* (21 October 2009) at paras. 100-03:

> 101. The Commission notes that in a number of decisions, it has established regulatory measures to safeguard customer information and to protect the privacy of consumers. In Telecom Decision 2006-15, as amended by the Governor in Council's *Order Varying Telecom Decision CRTC 2006-15*, P.C. 2007-532, 4 April 2007 (modified Telecom Decision 2006-15), the Commission considered that protecting the privacy of telecommunications service customers was increasingly important due to the advent of

98) In the view of PIAC/CAC, the Commission's conclusions in the ITMP framework reflects a broader privacy principle enshrined in the Section 7(i) policy objective of "protection of privacy of persons".

(III) The Bell Relevant Ads Program is a violation of the Commission's Confidential Customer Information rules

99) PIAC/CAC contend that the Bell Relevant Ads Program is a violation of the confidential customer information rules.

100) The Commission has, in furtherance of the telecommunications policy objective of the "protection of the privacy of persons" in Section 7(i) of the *Telecommunications Act*, imposed confidentiality obligations on Canadian carriers in respect of both tariffed and forborne telecommunications services (except forborne mobile wireless services that are not switched, such as paging).[75] These obligations, and prescribed language, are reflected in the Canadian carriers' tariffs or in the customer service contracts, as the case may be.

101) The Commission describes the confidential customer information rules as follows.

> new technologies and the emergence of electronic commerce, which enable information to be more easily processed, rearranged, and exchanged.
>
> 102. The Commission notes that parties who argued against privacy provisions did so because they claimed the existence of PIPEDA made additional provisions unnecessary. However, the Commission considers that, as a result of paragraph 7(*i*) of the Act, its role with respect to the protection of privacy in the telecommunications industry is complementary to that of the Office of the Privacy Commissioner of Canada. The Commission considers that in the circumstances of this proceeding, similar to the findings made in Telecom Decision 2003-33 and modified Telecom Decision 2006-15, it would be appropriate to impose a higher standard than that available under PIPEDA in order to provide a higher degree of privacy protection for customers of telecommunications services.
>
> 103. In light of the above, the Commission finds it appropriate to establish privacy provisions in order to protect personal information. The Commission therefore directs all primary ISPs, as a condition of providing retail Internet services, not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information.

[75] See Telecom Decision CRTC 2003-33 - *Confidentiality provisions of Canadian carriers* (30 May 2003), as amended by Telecom Decision CRTC 2003-33-1, at para. 1.

> The confidentiality provisions, which protect the confidentiality of customer information, are incorporated in the tariffs of the ILECs and imposed on Canadian carriers in respect of services (except for non-public-switched wireless services) from which the Commission has forborne. The Commission considers that these provisions are even more relevant today than when they were first implemented, due to the advent of new technologies and the emergence of electronic commerce, which allow information to be easily processed, re-arranged and exchanged. [76]

102) Bell's tariff (which applies to wireline services) (and the parallel language that is required to be in Bell Mobility's wireless service contracts) is determinative of what customer information should be confidential, and also determinative of what is the proper purpose of confidential customer information.

103) Confidential customer information is "all information kept by the Company regarding the customer, other than the customer's name, address and listed telephone number".[77]

104) Unless a customer provides express consent or disclosure is pursuant to a legal power, all confidential customer information kept by Bell may not be disclosed by the Bell to anyone except in very narrow service-related or law enforcement related circumstances.[78] That includes disclosure of information to affiliates involved in supplying the customer with telecommunications and/or broadcasting services.[79]

105) The Bell Relevant Ads Program involves extensive information (described above) about Bell's customers, beyond specific customers' names, addresses and listed telephone numbers. Because Bell has not obtained the express consent of its customers, the Bell Relevant Ads Program is a violation of the confidential customer information rules. Specifically, the confidential customer information rules do not allow Bell to sell aggregated data of its customers, and do not allow Bell to give confidential customer information to its retail affiliate, The Source.

(IV) The Bell Relevant Ads Program is a violation of Section 36 of the *Telecommunications Act*

106) PIAC/CAC contend that the Bell Relevant Ads Program is a violation of Section 36 of the *Telecommunications Act* because Bell is using information gleaned from its role as providing telecommunications service for the unapproved purpose of marketing,

---

76 *Ibid*. at para. 24.

77 CRTC 6716, Art. 11.

78 *Ibid.*

79 CRTC 6716, Art. 11.1; Telecom Decision 2003-33 at paras. 24-29.

and because the Bell Relevant Ads Program is a conflict of interest for Bell as a vendor of telecommunications services *and* a vendor of advertising and advertising services.

107) Section 36 prohibits Canadian carriers from controlling the content or influencing the meaning or purpose of telecommunications carrier by it for the public, except with prior Commission approval.

> Content of messages
>
> **36.** Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public.

108) Bell, through its Bell Mobility division, is a "Canadian carrier", that is, a "telecommunications common carrier" – "a person who owns or operates a transmission facility used by that person or another person to provide telecommunications services to the public for compensation".[80]

109) Bell is gathering subscriber information gleaned from the telecommunications of its customers which its customers compensate Bell for carrying – for advertising and marketing purposes as part of Bell's four-screen strategy that emphasizes advertising revenue. The Commission has not previously approved Bell's use of telecommunications carried by it for that purpose, and PIAC/CAC is not aware of any pending request by Bell for Section 36 approval.

110) PIAC/CAC contend that this collection, use and processing influences the meaning and purpose of telecommunications carried by it for the public. Bell's action risks Bell taking measures, for example, which may favour collection of information that otherwise degrade the signal or response time of the telecommunications it is primarily required to deliver, unchanged.

111) The Bell Relevant Ads Program, which, as stated earlier, appears to be part of a broader four-screen strategy that emphasizes advertising revenue, puts Bell in a conflict of interest between its role as a provider of telecommunications services to the public for compensation and its desired role as a purveyor of customer information for advertising and marketing services to the private sector for compensation.

[80] *Telecommunications Act*, Section 2(1).

112) PIAC/CAC therefore contend that Bell is in violation of Section 36 of the *Telecommunications Act* as it has not sought prior Commission approval of this new purpose to its telecommunications service, an approval which PIAC/CAC oppose, both for the reasons in this section and for the other reasons provided in this application.

4. THE IMPORTANCE OF COMMISSION INTERVENTION

113) The Bell Relevant Ads Program is a critical test of the Commission's privacy rules and regulatory powers on which, in the words of the Privacy Commissioner, "Canadians depend to protect privacy"[81] - in the face of an unprecedented and unsolicited collection, use and disclosure of information about Canadians, and in light of a recognized need for telecommunications-specific privacy rules.

114) With the rise in smartphone adoption and use and the push toward an all IP-architecture through which more and more Canadians experience more and more of their lives, the risk of a major data breach from a program such as Bell's are too great to not give Canadians the full benefit of protection from data collection and use by their telecommunications service providers and BDUs.

115) High-profile data breaches, such as the recent data breach of at least 70 million Target customers' information, (including names, mailing addresses, telephone numbers and email addresses)[82], warrant serious scrutiny by the Commission of the practice of data collection and use by a telecommunications service provider (with broadcasting undertaking, and broadcasting distribution undertaking and retail affiliates).

The Need for Telecommunications-specific Privacy Rules

116) On several occasions the Commission has, under Section 7(i) telecommunications policy objective of contributing "to the protection of privacy of persons", recognized the need for a higher degree of privacy protection than provided by PIPEDA.

---

81 *Infra* note 86.

82 "U.S. states launch joint probe as Target data-breach toll mounts", *The Globe and Mail* (10 January 2014).

117) For example, in the Commission's update to the customer confidential information rules the Commission noted:

> [...] that the PIPED Act sets out regulations and standards relating to the privacy of personal information. However, the Commission also notes that its jurisdiction in this matter stems not from the PIPED Act, but from the *Telecommunications Act*, and that in exercising its discretionary powers pursuant to the *Telecommunications Act*, it may apply different standards than those contemplated by the PIPED Act.[83]

118) Also, in the Commission's ITMP framework:

> The Commission notes that parties who argued against privacy provisions did so because they claimed the existence of PIPEDA made additional provisions unnecessary. However, the Commission considers that, as a result of paragraph 7(*i*) of the Act, its role with respect to the protection of privacy in the telecommunications industry is complementary to that of the Office of the Privacy Commissioner of Canada. The Commission considers that in the circumstances of this proceeding, similar to the findings made in Telecom Decision 2003-33 and modified Telecom Decision 2006-15, it would be appropriate to impose a higher standard than that available under PIPEDA in order to provide a higher degree of privacy protection for customers of telecommunications services.[84]

119) By the same token, the Privacy Commissioner has recognized its office's limited authority to only make "soft recommendations"[85], and has also recognized its office's own lack of enforcement powers.

> The days of soft recommendations with few consequences for non-compliance are no longer effective in a rapidly changing environment where privacy risks are on the rise.[86]

---

83 Telecom Decision CRTC 2003-33 - *Confidentiality provisions of Canadian carriers* (30 May 2003), as amended by Telecom Decision CRTC 2003-33-1, at para. 24.

84 Telecom Regulatory Policy CRTC 2009-657 - *Review of the Internet traffic management practices of Internet service providers* (21 October 2009) at para. 102.

85 The Office of the Privacy Commissioner of Canada, "The Case for Reforming the *Personal Information Protection and Electronic Documents Act"* (May 2013) (footnotes omitted).

> Under the Act, the Privacy Commissioner of Canada is an "administrative investigator," with a range of powers, including the ability to initiate her own investigations and audits (with reasonable grounds), and the power to compel evidence and enter premises when conducting investigations. The Commissioner may seek resolution through negotiation, persuasion and mediation. While the Commissioner may encourage compliance by naming respondent organizations when it is deemed in the public interest, she herself has no direct enforcement powers. The Commissioner can only, in certain circumstances, apply to the Federal Court to have the Court hear certain matters raised in complaints to her Office; order the respondent to take action to correct its practices; or award damages to the complainant.

120) The Privacy Commissioner has also recognized the important role that the CRTC has to play in protecting Canadians' privacy.[87]

121) As the Privacy Commissioner has noted in previous submissions to the CRTC:

> while the OPC and CRTC's roles are complementary, they are not redundant, given the difference in functions and powers. PIPEDA is a statute of general application that applies to diverse industries, while the *Telecommunications Act* is sector-specific and enables the CRTC to create specific guidelines and regulations to address concerns within the industry.[88]

122) In a submission to the CRTC in its review of regulatory measures associated with confidential customer information and privacy, the Privacy Commissioner stated that "The CRTC's rules and regulatory powers represent an important control Canadians depend on to protect personal information."[89]

123) In a submission to the CRTC in the ITMP framework proceeding[90], the Privacy Commissioner stated:

i) The CRTC has a statutory obligation and recognized expertise to protect privacy.

ii) PIPEDA provides a basic standard for privacy protection: The CRTC may set higher, industry specific guidelines.

iii) Canadians care about personal privacy and are entitled to know how their personal information is being handled and protected.[91]

---

86 *Ibid.*

87 Final reply of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) regarding Review of the Internet traffic management practices of Internet service providers (July 2009).

88 Comments in Response to Consultation on Matters Related to 9-1-1 Service, Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunications Commission (CRTC) (1 March 2013) at para. 11 (footnotes omitted).

89 Review of the regulatory measures associated with confidential customer information and privacy - Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC), at paras. 14 and 15.

90 Telecom Public Notice CRTC 2008-19 - *Review of the Internet traffic management practices of Internet service providers* (20 November 2008).

91 Final reply of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) regarding Review of the Internet traffic management practices of Internet service providers (July 2009).

124) The Privacy Commissioner therefore concluded:

> Canadians have mounting concerns about the preservation of privacy rights. They are entitled to have clear, easily accessible, and meaningful safeguards of their personal information, and how it is managed by ISPs implementing traffic management practices. They expect that their personal information will not be misused, and will be treated with a high standard of care by the organizations they choose to do business with, and that the public bodies tasked with the duty to protect their privacy, not hesitate to do so.[92]

125) The Privacy Commissioner has encouraged the CRTC to develop standards: "The OPC encourages the CRTC to develop benchmark privacy guidance that meshes existing regulation of broadcast/online advertising with protections for confidential consumer information."[93]

126) Although the Privacy Commissioner has also developed baseline standards for online behavioural advertising - the Commissioner's *Online Behavioural Advertising Guidelines*[94] (the "**OBA Guidelines**"), PIAC/CAC contend these are insufficient because they contain discretionary ("should") obligations framed as guidelines and not rules, and furthermore because the Privacy Commissioner has noted they are "not intended to apply to ... advertising in the mobile context."[95]

127) Also, although the Privacy Commissioner has made findings in the past in respect of Bell's adherence to PIPEDA, the Privacy Commissioner has also recognized the potential for higher standards to be applied by the CRTC under the *Telecommunications Act*.

128) PIAC/CAC contend that the Commission's customer confidentiality rules, the ITMP framework and the privacy principle expressed therein, and Section 36 of the *Telecommunications Act* reflect such higher standards, and prohibit Bell from using customer information for behavioural marketing.

---

92 Final reply of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) regarding Review of the Internet traffic management practices of Internet service providers (July 2009).

93 *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing* (May 2011) at 32.

94 Office of the Privacy Commissioner of Canada, *Privacy and Online Behavioural Advertising*, (June 2012).

95 Office of the Privacy Commissioner of Canada, *Policy Position on Online Behavioural Advertising*, (2012).

The Bell Privacy Policy is Insufficient to Protect Canadians' Privacy

129) PIAC/CAC contend that the Bell Privacy Policy, found at Appendix "C", is insufficiently specific and detailed to protect Canadians' privacy and an insufficient defence to the violations alleged herein of the privacy obligations reflected in the *Telecommunications Act* and in Commission policy.

130) The Bell Privacy Policy appears designed to meet minimum consent requirements in PIPEDA. For reasons discussed above, a higher standard is needed to protect Canadians' against the collection and use of their information for behavioural marketing by their telecommunications service provider.

131) PIAC/CAC contend that that higher standard is already reflected in the Commission's confidential customer information rules, the ITMP framework and the privacy principle expressed therein, and Section 36 of the *Telecommunications Act*, each in furtherance of the telecommunications policy objective of "the protection of privacy of persons".

132) Even under PIPEDA, Bell's privacy policy falls short of providing the required specificity or detail to allow a customer to determine the "Relevant Ads" program's sweeping scope and actual operation. Without this specificity and detail, any consent, implied or explicit, is obviated.[96]

[96] See: *Personal Information Protection and Electronic Documents Act*, RSC 2000, c 5, Schedule 1, Principles 4.3.2 - 4.3.4.

> **4.3.2**
>
> The principle requires "knowledge and consent". 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.
>
> **4.3.3**
>
> An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.
>
> **4.3.4**
>
> The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would

133) The role of information in establishing meaningful consent is illustrated by two pertinent findings by the Privacy Commissioner, one in respect of Bell, and one in respect of Google.

134) In the case of Google[97], the Privacy Commissioner found that Google had violated the Privacy Commissioner's OBA Guidelines and the requirement for meaningful consent for OBA when Google inserted a cookie in an Internet viewer's browser, after the viewer had visited specific sites relating to a specific health condition which then led to the targeted delivery of ads relating to the viewer's specific health condition.

135) In the case of Bell[98], the Privacy Commissioner found a violation by Bell of PIPEDA Principle 4.3.2 in previous versions of Bell's Internet Service Agreement and the Bell Internet Dial-up Service Agreement which indicated that users are informed in a general way of the possibility of Bell monitoring their use of Bell's networks.

> 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

---

> generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

97 PIPEDA Report of Findings #2014-001 - *Use of sensitive health information for targeting of Google ads raises privacy concerns* (14 January 2014).

> 23. Our Office is of the view that meaningful consent is required for the delivery of OBA. As stated in our Office's OBA guidelines, implied or opt-out consent for OBA purposes may be acceptable provided that the information collected and used is limited, to the extent practicable, to **non-sensitive** information (avoiding sensitive information such as medical or health information).
>
> 24. The complainant was searching information related to a medical device used to treat sleep apnea. Given that this complaint relates to personal health information (i.e. online activities and viewing history of health related websites), our Office is of the view that such information is sensitive. Therefore, implied consent for the collection or use of the complainant's sensitive personal health information for the purpose of delivering ads based on the complainant's online behaviour is not appropriate, and express consent is required.
>
> 25. Since Google did not seek express consent in the circumstances, we are of the view that in this context, Google has contravened Principles 4.3 and 4.3.6 of the Act. (emphasis original)

98 PIPEDA Case Summary #2009-010 - Report of Findings - Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection (September 2009).

> 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. […][99]

136) Both cases highlight the potential for improper data collection and use, and an incomplete understanding by Canadians of how their online behaviour (in addition to other telecommunications activities) could be used in unclear ways. In light of the scale and scope of Bell as telecommunications service provider (and broadcasting undertaking, broadcasting distribution undertaking, and retailer), and in recognition of how the Commission has imposed higher standards than required by PIPEDA, PIAC/CAC contend that Commission intervention is required in respect of the Bell Relevant Ads Program.

5. NATURE OF DECISION SOUGHT

137) PIAC/CAC contend that Bell is overstepping its role of providing telecommunications services to the public for compensation by pursuing a business model that also includes using and disclosing customer information, gained through the consumption of Bell's telecommunications services, for advertising and marketing purposes.

138) Section 7(i) of the *Telecommunications Act* established "the protection of privacy of persons" as a telecommunications policy objective.

139) The Commission has the authority to address privacy in respect of wireless services via section 24 of the *Telecommunications Act*, and also via Section 32(g) of the *Telecommunications Act.*

140) Although the Commission has forborne from the exercise of some of its power and the performance of some of its duties under Section 24 of the *Telecommunications Act*, it did not relinquish its authority to deal with confidentiality issues or to impose any conditions that may be necessary in the future.[100]

---

99 *Ibid.* at para. 51.

100 Telecom Decision CRTC 94-15, *Regulation of wireless services*, 12 August 1994; Telecom Decision CRTC 96-14, *Regulation of mobile wireless telecommunications services,* 23 December 1996 (Telecom Decision 96-14); Telecom Decision CRTC 2010-445 - *Modifications to forbearance framework for mobile wireless data services* (30 June 2010).

141) The Commission has established privacy protections in respect of confidential customer information and ITMPs, and Section 36 of the *Telecommunications Act* prohibits Canadian carriers from influencing the meaning or purpose of telecommunications carried by it for the public.

142) PIAC/CAC therefore request that the Commission exercise its authority under Sections 24 and 32(g) of the *Telecommunications Act,* in line with the privacy objective in the *Telecommunications Act* and the privacy principles found in the Commission's confidential customer information rules and ITMP framework, to stop the collection and use of information about Canadians by Bell for the purposes of behavioural advertising.

143) In light of the Commission's special position and role in the protection of Canadian's privacy, as acknowledged by the Privacy Commissioner, and in light of the concerns raised about the Bell Relevant Ads Program, PIAC/CAC request that the Commission:

(i) Declare that the Bell Relevant Ads Program is contrary to the *Telecommunications Act*;

(ii) Declare that the Bell Relevant Ads Program violates the Commission's confidential customer information rules;

(iii) Declare that the Bell Relevant Ads Program is contrary to the ITMP framework; or contrary to the privacy principle reflected in the ITMP framework and in the *Telecommunications Act*;

(iv) Declare that the Bell Relevant Ads Program violates Section 36 of the *Telecommunications Act*;

(v) Prohibit Bell from collecting and using customer information for advertising and marketing purposes as set out in the Bell Relevant Ads Program.

(vi) Initiate a larger, follow-up proceeding to examine the data collection, use and disclosure practices of all other telecommunications service providers and BDUs; and

(i) grant PIAC/CAC their costs of making this Part 1 application in accordance with Section 56 of the *Telecommunications Act.*

144) This primary relief is appropriate as only prohibition of the practice will bring about accordance with the *Telecommunications Act*.

145) In the alternative if the Commission denies the request by PIAC/CAC to prohibit Bell from using customer information for advertising and marketing purposes as set out in the Bell Relevant Ads Program, PIAC/CAC request that the Commission direct Bell to make the Bell Relevant Ads program entirely opt-in; and to fully disclose all details of the collection, use and disclosure of the personal information to users in their privacy policies and related documents.

146) Given the size and scale of Bell and its reach into Canadians lives, PIAC/CAC submit that the Commission should take this opportunity to confirm the role of telecommunications common carriers as neutral providers of telecommunications services to the public, and not providers of customer information to themselves and to other advertisers.

6. SERVICE

147) Electronic service of this application has been made to the respondent, Bell.

7. NOTICE

148) This application is made by the Public Interest Advocacy Centre, c/o Geoffrey White, Counsel, Public Interest Advocacy Centre, One Nicholas Street, Suite 1204, Ottawa, Ontario K1N 7B7.

149) A copy of this application may be obtained by sending a request to piac@piac.ca. A copy of this application has also been posted to PIAC's website at http://www.piac.ca.

150) TAKE NOTICE that pursuant to section 25, and, as applicable section 26 of the *Canadian Radio-television and Telecommunications Commission Rules of Practice and* Procedure, any respondent or intervener is required to mail or deliver or transmit by electronic mail its answer to this application to the Secretary General of the Canadian Radio-television and Telecommunications Commission ("**Commission**"), Central Building, 1 Promenade du Portage, Gatineau (Québec) J8X 4B1, and to serve a copy of the answer on the applicant within 30 days of the date that this

application is posted on the Commission's website or by such other date as the Commission may specify.

151) Service of the copy of the answer on the applicant may be effected by personal delivery, by electronic mail, or by ordinary mail. In the case of service by personal delivery, it may be effected at the address set out above.

152) If a respondent does not file or serve its answer within the time limit prescribed, the application may be disposed of without further notice to it.

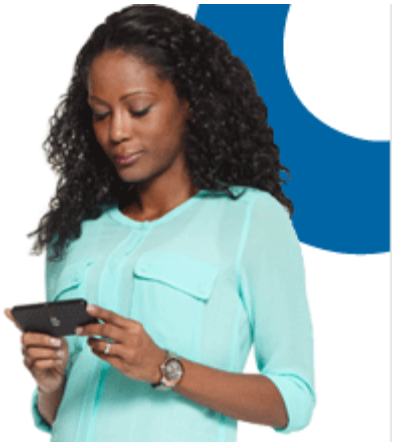
End of document

Appendix "A" – The Bell Relevant Ads Program Notice

Bell

View in browser

Important notice about how Bell uses information.



Why am I getting this notice?

Your privacy is an important priority at Bell, and so is providing an experience that best meets your needs. Our Privacy Policy (available at bell.ca/privacy) informs you about information we collect and how we use it. Today, we want to tell you about some important updates relating to new uses of information.

Starting on November 16, 2013, Bell will begin using certain information about your account and network usage for select purposes, such as continuing to improve network performance and product offers through new business and marketing reports, making some of the ads and marketing partner offers you see more relevant to you, and providing

increased levels of fraud detection and prevention. We will not share any information that identifies you personally outside of Bell Canada and its affiliates. If you do not want us to use this information for these purposes, you can let us know by visiting bell.ca/relevantads. This supplements our Privacy Policy.

What information are we talking about?

Bell will use the following categories of information:

Network usage information, such as:

- Web pages visited from your mobile device or your Internet access at home. This may include search terms that have been used.
- Location
- App and device feature usage
- TV viewing
- Calling patterns

Account information:

- Information about your use of Bell products and services (such as device type, postal code, payment patterns and language preference)
- Demographic information, such as gender or age range

Is my information shared?

No, under these new programs, we will not share any information that identifies you personally outside of Bell Canada and its affiliates.

How information will be used.

To create business and marketing reports.

Description	Example
We will combine network usage information and account information in a way that does not personally identify you. We will use this information to prepare business and marketing reports that we may use ourselves or share with others.	We may generate a report that shows 5,000 mobile users downloaded a gaming application in a month, and 80% of them were

	18-25 years old.

For other companies to create business and marketing reports.	
Description	**Example**
We may also share information with other companies in a way that does not personally identify you. We will allow these companies to produce limited business and marketing reports.	Using information from Bell and other mobile carriers, a company may generate a report that shows how many mobile users were active along a certain parade route.

To make ads you see more relevant.	
Description	**Example**
When you use the Internet on your mobile device, laptop, computer or TV, you often see unfiltered, random ads on websites and within apps. We would like to use certain network usage information and account	A hotel chain may want to only advertise their Montréal location to out-of-town mobile users. Bell may exclude

information to make the ads you see more relevant to you. These ads may be from Bell or from third parties, however Bell will not share any of your personal information with a third party as part of placing a third party ad.	Montréal users on the hotel's behalf when delivering the ad (without sharing personal information).

Your choices.

Description	
You will receive unfiltered and random ads whether you participate or not, but under this program, ads may be more relevant to you.	If you do not want us to use your information for any of the purposes described above, please let us know at any time by visiting bell.ca/relevantads

End of document

Appendix "B" - Research on Canadians' Attitudes toward Privacy

Excerpts from Privacy Commissioner comments to CRTC on ITMPs[101]

> According to the Interactive Advertising Bureau of Canada's representations to our Consultation process, surveys indicate that consumers do not want to pay for content on the Internet and that they are willing to be exposed to online advertising in order to receive free online content. A Canadian Marketing Association 2009 study noted that 50% of Canadians were "somewhat uncomfortable" with marketers using browsing information to serve more relevant ads. Interestingly, according to this study, approximately 51% of Canadians delete their cookies at least once a month.
>
> A joint Berkeley and University of Pennsylvania study found that consumers were more persuaded by the benefits of behavioural advertising if there was more transparency, consumer choice, and data retention limits.
>
> KPMG recently issued its Consumer and Convergence Report for 2011. The report notes that 46% of Canadians were "somewhat willing" to have their online usage tracked by advertisers, particularly when tracking provided a "payoff" (i.e. free services). This number is up from 36% in 2008. The percentage of Canadians who were "not at all willing" dropped from 49% in 2008 to 38%.

Excerpts from Privacy Commissioner's Report on 2010 Consultation[102]

> ***General attitudes toward privacy***
> A 2009 EKOS survey commissioned by our Office found that 90% of Canadians are concerned about the impacts of new technology. While individuals may not be aware of certain privacy risks or consciously accept a trade-off to their privacy, Canadians still have high expectations for privacy, including online, and worry about how their personal information is being used, especially if it involves transborder data flows.
>
> People between the ages of 45 and 65 are particularly likely to be concerned about the privacy impact of new technologies, while those under 25 are less likely to express high levels of concern about the issue. Canadians under 25 are also less likely to be concerned about off-shore processing and storage of their personal information.
>
> Overall, 98% of all Canadians believe that it is important to have strong privacy laws.
>
> ***Attitudes toward online tracking and targeting***
> According to a 2009 survey conducted by the Public Interest Advocacy Centre (PIAC) on online behavioural tracking, nearly 75% of respondents were either not very comfortable or not comfortable at all with tracking-based advertising. Awareness of tracking devices and techniques was split 50-50 between individuals who were aware and those who were

---

101 Final reply of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) regarding Review of the Internet traffic management practices of Internet service providers (July 2009) (footnotes omitted).

102 Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing (May 2011), online: https://www.priv.gc.ca/resource/consultations/report_201105_e.asp (footnotes omitted).

not aware of such techniques. The study found that individuals tended to be more comfortable with online tracking for customer service or advertising purposes if done by companies with which they have had prior dealings.[16] In a study conducted on behalf of the Canadian Marketing Association (CMA) in 2009 on behavioural advertising, it was noted that 50% of Canadians were "somewhat uncomfortable" with marketers using browsing information to serve more relevant ads.[17] In one study discussed during a panel discussion in Montreal, it was noted that individuals end to become more comfortable with behavioural advertising once it is explained to them.

Attitudes toward geolocational privacy

In terms of location data, Natural Resources Canada conducted a survey concerning Canadians' views on privacy and the use of geospatial information. Some of the key conclusions in the study were that Canadians are fairly careful about sharing their location-based information and that control over the information being shared and the context are key drivers of individuals' comfort when faced with sharing location-linked personal information. Leading to higher levels of discomfort are "situations where information is being linked to one's real time location, being used for targeted marketing, where there is little or no control, being shared with the private sector or general public and for reasons related to economic activity…." Approximately half of the respondents did not perceive any benefits to location-tracking technology or were unsure what benefits it may provide.

End of document

Appendix "C" – Bell Privacy Policy

(Downloaded Monday, December 16, 2013)

Bell Privacy Policy

Last revised February 2012

The Bell Privacy Policy reflects the requirements of the Personal Information Protection and Electronic Documents Act and incorporates the ten principles of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), which was published in March 1996 as a National Standard of Canada.

Table of Contents

Introduction

The Bell companies provide a full range of services to meet the communications needs of consumers including wireless, high-speed internet, satellite and IP television, local and long distance wireline services as well as radio, television and digital media services.

The Bell Companies have long been committed to maintaining the accuracy, confidentiality, security and privacy of customer and employee personal information. This is reflected in existing privacy and confidentiality provisions found in various Bell policies, agreements and in applicable service rules approved by regulatory agencies over the years. It is also reflected in the high regard and trust with which customers and employees view the management of personal information by the Bell companies.

In March 1996, the new Canadian Standards Association *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96 (the "CSA Code"), was published as a National Standard of Canada. In August 2000, the Bell companies revised the *Bell Privacy Policy* (formerly, the *Bell Code of Fair Information Practices),* to describe in detail how we subscribe to the principles of the CSA Code and the requirements of the *Personal Information Protection and Electronic Documents Act*, which came into force in 2001.

The *Bell Privacy Policy* is a formal statement of principles and guidelines concerning the minimum requirements for the protection of personal information provided by the Bell companies to our customers and employees. The objective of the *Bell Privacy Policy* is responsible and transparent practices in the management of personal information, in accordance with the National Standard and federal legislation.

The Bell companies will continue to review the *Bell Privacy Policy* and privacy-related information made publicly available to make sure it is relevant and remains current with changing technologies and laws and the evolving needs of the Bell companies, our customers and employees. This version of the *Bell Privacy Policy* was updated in May 2011.

Scope and Application

The 10 principles that form the basis of the *Bell Privacy Policy* are interrelated and Bell shall adhere to the 10 principles as a whole. Each principle must be read in conjunction with the accompanying commentary. As permitted by the CSA Code, the commentary in the *Bell Privacy Policy* has been tailored to reflect personal information issues specific to the Bell companies.

The scope and application of the *Bell Privacy Policy* are as follows:

- The *Bell Privacy Policy* applies to the various Bell companies offering communications services including wireless, high-speed internet, satellite and IP

television, local and long distance wireline services as well as radio, television and digital media services, and our various retail locations (and any successor company or companies of the above, as a result of corporate reorganization or restructuring). The *Bell Privacy Policy* also applies to the Ontario and Québec operations of Bell Aliant. Any time you do business with any of the Bell companies, or with anyone acting as an agent on our behalf, you are protected by the rights and safeguards contained in the *Bell Privacy Policy.*

- The *Bell Privacy Policy* applies to personal information about customers and employees of the Bell companies that is collected, used or disclosed by these companies.

- The *Bell Privacy Policy* applies to the management of personal information in any form whether oral, electronic or written.

- The *Bell Privacy Policy* does not impose any limits on the collection, use or disclosure of the following information by the Bell companies:

  a) information that is publicly available, such as a customer's name, address and telephone number when listed in a directory or made available through directory assistance;
  b) name, title or business address or telephone number of an employee of an organization; or
  c) other information about a customer or an employee that is publicly available and is set out in Regulations made pursuant to the *Personal Information Protection and Electronic Documents Act.*

- The *Bell Privacy Policy* does not apply to customers that are not individuals, such as corporate customers; however, information collected from such customers is protected by other Bell policies and practices and by applicable contractual terms.

- The application of the *Bell Privacy Policy* is subject to the requirements or provisions of the *Personal Information Protection and Electronic Documents Act*, the Regulations made there under, and any other applicable legislation, regulations, tariffs or agreements (such as collective agreements), or the order of any court or other lawful request.

Definitions

Collection - the act of gathering, acquiring, recording or obtaining personal information from any source, including third parties, by any means.

Consent - voluntary agreement with the collection, use and disclosure of personal information for defined purposes. Consent can be either express or implied and can be provided directly by the individual or by an authorized representative. Express

consent can be given orally, electronically or in writing but is always unequivocal and does not require any inference on the part of the Bell companies. Implied consent is consent that can reasonably be inferred from an individual's action or inaction.

Customer - an individual who
- uses, or applies to use, the products or services of a Bell company;
- corresponds with a Bell company; or
- enters a contest sponsored by a Bell company.

Disclosure - making personal information available to a third party.

Employee - an employee or pensioner of a Bell company.

Personal information - information about an identifiable individual but not aggregated information that cannot be associated with a specific individual.

- For a **customer**, such information includes a customer's credit information, billing records, service and equipment records, and any recorded complaints.
- For an **employee**, such information includes information found in personal employment files, performance appraisals and medical and benefits information.

Third party - an individual other than the customer or his agent, or an organization other than the Bell companies or their agents.

Use - the treatment, handling, and management of personal information by the Bell companies and their agents.

Principle 1 - Accountability

The Bell companies *are responsible for personal information under their control and shall designate one or more persons who are accountable for the* companies' *compliance with the following principles.*

1.1 Responsibility for ensuring compliance with the provisions of the *Bell Privacy Policy* rests with the senior management of the Bell companies, which shall designate one or more persons to be accountable for compliance with the *Bell Privacy Policy*. Other individuals within Bell companies may be delegated to act on behalf of the designated person(s) or to take responsibility for the day-to-day collection and processing of personal information.

1.2 The Bell companies shall make known, upon request, the title of the person or persons designated to oversee the companies' compliance with the *Bell Privacy Policy*.

The Bell companies have designated the Bell Privacy Ombudsman to oversee compliance with the *Bell Privacy Policy*. The Bell Privacy Ombudsman can be contacted at:

The Office of the Bell Privacy Ombudsman
160 Elgin Street
Ottawa, ON K2P 2C4
privacy@bell.ca

1.3 The Bell companies are responsible for personal information in their possession or control, including information that has been transferred to a third party for processing. The Bell companies shall use appropriate means to provide a comparable level of protection while information is being processed by a third party (see Principle 7).

1.4 The Bell companies have implemented policies and procedures to give effect to the *Bell Privacy Policy*, including:

a) implementing procedures to protect personal information and to oversee the company's compliance with the *Bell Privacy Policy*;
b) establishing procedures to receive and respond to inquiries or complaints;
c) training and communicating to staff about the company's policies and practices; and
d) developing public information to explain the company's policies and practices.

Principle 2 - Identifying Purposes for Collection of Personal Information

The Bell companies shall identify the purposes for which personal information is collected at or before the time the information is collected.

2.1 The Bell companies collect personal information only for the following purposes:

a) to establish and maintain responsible commercial relations with customers and to provide ongoing service;
b) to understand customer needs and preferences, and determine eligibility for products and services;
c) to recommend particular products & services to meet customer needs;
d) to develop, enhance, market or provide products and services;
e) to manage and develop their business and operations, including personnel and employment matters; and
f) to meet legal and regulatory requirements.

Further references to "identified purposes" mean the purposes identified in this Principle 2.

2.2 The Bell companies shall specify orally, electronically or in writing the identified purposes to the customer or employee at or before the time personal information is collected. Upon request, persons collecting personal information shall explain these identified purposes or refer the individual to a designated person within the Bell companies who shall explain the purposes.

2.3 Unless required by law, the Bell companies shall not use or disclose, for any new purpose, personal information that has been collected without first identifying and documenting the new purpose and obtaining the consent of the customer or employee.

Principle 3 - Obtaining Consent for Collection, Use or Disclosure of Personal Information

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

3.1 In certain circumstances personal information can be collected, used or disclosed without the knowledge and consent of the individual. For example, the Bell companies may collect or use personal information without knowledge or consent if it is clearly in the interests of the individual and consent cannot be obtained in a timely way, such as when the individual is a minor, seriously ill or mentally incapacitated.

The Bell companies may also collect, use or disclose personal information without knowledge or consent if seeking the consent of the individual might defeat the purpose of collecting the information such as in the investigation of a breach of an agreement or a contravention of a federal or provincial law.

The Bell companies may also use or disclose personal information without knowledge or consent in the case of an emergency where the life, health or security of an individual is threatened.

The Bell companies may disclose personal information without knowledge or consent to a lawyer representing the companies, to collect a debt, to comply with a subpoena, warrant or other court order, or as may be otherwise required by law.

3.2 In obtaining consent, the Bell companies shall use reasonable efforts to ensure that a customer or employee is advised of the identified purposes for which personal information will be used or disclosed. Purposes shall be stated in a manner that can be reasonably understood by the customer or employee.

3.3 Generally, the Bell companies shall seek consent to use and disclose personal information at the same time it collects the information. However, the Bell

companies may seek consent to use and disclose personal information after it has been collected but before it is used or disclosed for a new purpose.

3.4 The Bell companies will require customers to consent to the collection, use or disclosure of personal information as a condition of the supply of a product or service only if such collection, use or disclosure is required to fulfill the identified purposes.

3.5 In determining the appropriate form of consent, the Bell companies shall take into account the sensitivity of the personal information and the reasonable expectations of its customers and employees.

3.6 In general, the use of products and services by a customer, or the acceptance of employment or benefits by an employee, constitutes implied consent for the Bell companies to collect, use and disclose personal information for all identified purposes.

3.7 A customer or employee may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Customers and employees may contact the Bell companies for more information regarding the implications of withdrawing consent.

Principle 4 - Limiting Collection of Personal Information

The Bell companies shall limit the collection of personal information to that which is necessary for the purposes identified by the company. The Bell companies shall collect personal information by fair and lawful means.

4.1 The Bell companies collect personal information primarily from their customers or employees.

4.2 The Bell companies may also collect personal information from other sources including credit bureaus, employers or personal references, or other third parties that represent that they have the right to disclose the information.

Principle 5 - Limiting Use, Disclosure and Retention of Personal Information

The Bell companies shall not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law. The Bell companies shall retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected.

5.1 In certain circumstances personal information can be collected, used or disclosed without the knowledge and consent of the individual. (see Principle 3.1)

5.2 In addition, the Bell companies may disclose a customer's personal information to:

a) another telecommunications company for the efficient and effective provision of telecommunications services;
b) a company involved in supplying the customer with communications or communications directory related services;
c) another person for the development, enhancement, marketing or provision of any of the products or services of the Bell Companies;
d) an agent retained by the Bell companies to evaluate the customer's creditworthiness
or to collect a customer's account;
e) credit grantors and reporting agencies;
f) a person who, in the reasonable judgment of the Bell companies, is seeking the information as an agent of the customer; and
g) a third party or parties, where the customer consents to such disclosure or disclosure is required by law.

5.3 In some cases, personal information collected by the Bell companies may be stored or processed outside of Canada to provide you with service or to support Bell operations, and may therefore be subject to the legal jurisdiction of these countries. The information is provided only after detailed contracts are set out with the companies that provide us with these services. Moreover, the information may only be used for the purposes of providing the services in question. When outsourcing certain functions, the Bell companies strive to minimize the personal information stored or processed outside of Canada. Wherever possible, the Bell Companies anonymize any personal information stored or processed outside Canada, such that the data cannot be associated with identifiable individuals. (See Principle 7 Security Safeguards)

5.4 The Bell companies may disclose personal information about its employees:

a) for normal personnel and benefits administration;
b) in the context of providing references regarding current or former employees in response to requests from prospective employers; or
c) where disclosure is required by law.

5.5 Only those employees of the Bell companies who require access for business reasons, or whose duties reasonably so require, are granted access to personal information about customers and employees.

5.6 The Bell companies shall keep personal information only as long as it remains necessary or relevant for the identified purposes or as required by law. Depending on the circumstances, where personal information has been used to make a decision about a customer or employee, the Bell companies shall retain, for a period of time that is reasonably sufficient to allow for access by the

customer or employee, either the actual information or the rationale for making the decision.

5.7 The Bell companies shall maintain reasonable and systematic controls, schedules and practices for information and records retention and destruction which apply to personal information that is no longer necessary or relevant for the identified purposes or required by law to be retained. Such information shall be destroyed, erased or made anonymous.

Principle 6 - Accuracy of Personal Information

Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

6.1 Personal information used by the Bell companies shall be sufficiently accurate, complete and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about a customer or employee.

6.2 The Bell companies shall update personal information about customers and employees as and when necessary to fulfill the identified purposes or upon notification by the individual.

Principle 7 - Security Safeguards

The Bell companies shall protect personal information by security safeguards appropriate to the sensitivity of the information.

7.1 The Bell companies shall protect personal information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction, through appropriate security measures. The Bell companies shall protect the information regardless of the format in which it is held.

7.2 The Bell companies shall protect personal information disclosed to third parties by contractual agreements stipulating the confidentiality of the information, the purposes for which it is to be used, limits on the number of persons whose job function requires access to the information, and the physical and procedural security measures required to safeguard that information.

7.3 All employees of the Bell companies with access to personal information shall be required as a condition of employment to respect the confidentiality of personal information.

Principle 8 - Openness Concerning Policies and Practices

The Bell companies shall make readily available to customers and employees specific information about its policies and practices relating to the management of personal information.

8.1 The Bell companies shall make information about its policies and practices easy to understand, including:

a) the title and address of the person or persons accountable for the companies' compliance with the *Bell Privacy Policy* (see Principle 1.2) and to whom inquiries or complaints can be forwarded (see "How to Contact Us" below);
b) the means of gaining access to personal information held by the companies (see Principle 9); and
c) a description of the type of personal information held by the companies, including a general account of its use.

8.2 The Bell companies shall make available information to help customers and employees exercise choices regarding the use of their personal information and the privacy-enhancing services available from the company.

Principle 9 - Customer and Employee Access to Personal Information

The Bell companies shall inform a customer or employee of the existence, use and disclosure of his or her personal information upon request and shall give the individual access to that information. A customer or employee shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

9.1 Upon request, the Bell companies shall afford to a customer or an employee a reasonable opportunity to review the personal information in the individual's file. Personal information shall be provided in understandable form within a reasonable time and at minimal or no cost to the individual.

9.2 In certain situations, the Bell companies may not be able to provide access to all of the personal information that they hold about a customer or employee. For example, the Bell companies may not provide access to information if doing so would likely reveal personal information about a third party or could reasonably be expected to threaten the life or security of another individual. Also, the Bell companies may not provide access to information if disclosure would reveal confidential commercial information, if the information is protected by solicitor-client privilege, if the information was generated in the course of a formal dispute resolution process, or if the information was collected in relation to the investigation of a breach of an agreement or a contravention of a federal or provincial law. If access to personal information cannot be provided, the Bell companies shall provide the reasons for denying access upon request.

9.3 Upon request, the Bell companies shall provide an account of the use and disclosure of personal information and, where reasonably possible, shall state the source of the information. In providing an account of disclosure, the Bell companies shall provide a list of organizations to which it may have disclosed personal information about the individual when it is not possible to provide an actual list.

9.3 In order to safeguard personal information, a customer or employee may be required to provide sufficient identification information to permit the Bell companies to account for the existence, use and disclosure of personal information and to authorize access to the individual's file. Any such information shall be used only for this purpose.

9.4 The Bell companies shall promptly correct or complete any personal information found to be inaccurate or incomplete. Any unresolved differences as to accuracy or completeness shall be noted in the individual's file. Where appropriate, the Bell companies shall transmit to third parties having access to the personal information in question any amended information or the existence of any unresolved differences.

9.5 A customer can obtain information or seek access to his or her individual file by contacting a designated representative at one of the Bell companies' business offices.

9.6 An employee can obtain information or seek access to his or her individual file by contacting his or her immediate supervisor within the applicable Bell company.

Principle 10 - Challenging Compliance

A customer or employee shall be able to address a challenge concerning compliance with the above principles to the designated person or persons accountable for the compliance of the Bell companies with the Bell Privacy Policy.

10.1 The Bell companies shall maintain procedures for addressing and responding to all inquiries or complaints from its customers and employees about the companies' handling of personal information.

10.2 The Bell companies shall inform their customers and employees about the existence of these procedures as well as the availability of complaint procedures (see "How to Contact Us" below).

10.3 The person or persons accountable for compliance with the *Bell Privacy Policy* may seek external advice where appropriate before providing a final response to individual complaints.

10.4 The Bell companies shall investigate all complaints concerning compliance with the *Bell Privacy Policy*. If a complaint is found to be justified, the company shall take appropriate measures to resolve the complaint including, if necessary, amending its policies and procedures. A customer or employee shall be informed of the outcome of the investigation regarding his or her complaint.

Questions or concerns about your privacy?

For more information on the Bell companies' commitment to privacy, contact any of the Bell companies at the number shown on your monthly bill, or visit our privacy pages at www.bell.ca/privacy.

If you have questions or concerns about your privacy, feel free to contact us and our customer service representatives will be delighted to speak to help you.

If you still have unresolved privacy concerns, you can write to:

The Office of the Bell Privacy Ombudsman
160 Elgin Street
Ottawa, Ontario K2P 2C4
privacy@bell.ca

If the Bell Privacy Ombudsman does not resolve the issue to your satisfaction, you can contact:

The Office of the Privacy Commissioner of Canada
112 Kent Street, Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario K1A 1H3
1-800-282-1376
www.priv.gc.ca

For copies of the *CSA Model Code for the Protection of Personal Information* contact:

Canadian Standards Association
5060 Spectrum Way, Suite 100
Mississauga, Ontario L4W 5N6
www.csa.ca