Date: 20080926

Docket: T-1385-07

Citation: 2008 FC 1086

Ottawa, Ontario, September 26, 2008

PRESENT: The Honourable Mr. Justice Zinn

BETWEEN:

DONALD PETER JOHNSON

Applicant

and

BELL CANADA

Respondent

REASONS FOR JUDGMENT AND JUDGMENT

[1] These reasons deal with the application of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA) to e-mail messages relating to an employee, sent or received by his co-workers, and which are stored on the employer's computers, servers and computer storage devices. The steps that an employer is required to undertake when responding to an access request by the subject of these e-mails is also considered.

BACKGROUND

[2] Mr. Johnson is a clerical employee of Bell Canada. On May 12, 2005, he sent an e-mail message to his direct manager requesting that he be provided with "e-mails concerning me in this company … from all sources". He subsequently narrowed his request for access to e-mails from the preceding two years, i.e. from May 12, 2003 to May 12, 2005. Faced with such a broad request, Bell Canada could have asked Mr. Johnson what e-mail messages he was really interested in seeing. Had it done so, it would have learned that his true interest was in seeing e-mail messages he believed had been sent by or to other employees of Bell Canada, some of whom occupied supervisory positions, and which concerned him. Bell Canada's position at the hearing was that Mr. Johnson, as the person making the request for access, had a duty to describe the documents he was requesting with more specificity.

[3] Prior to the expiry of the thirty day period for response to the access request that is set out in PIPEDA, Bell Canada advised Mr. Johnson that it required more time and that it would respond to his request no later than July 11, 2005. By letter of that date, Bell Canada did respond to Mr. Johnson, enclosing copies of some 280 e-mails comprising approximately 500 pages. Initially, some electronic messages were withheld pursuant to subsections 9(1) and 9(3)(e) of PIPEDA on the basis that their disclosure was likely to reveal personal information about a third party or threaten the security of another. Following the involvement of the Office of the Privacy Commissioner, the excluded messages were subsequently provided to Mr. Johnson in a redacted format.

[4] Bell Canada, adopted what I would describe as a focused process to extract the e-mails requested by Mr. Johnson. It did not conduct a search of the data on its servers, back-ups or every hard drive in the organization. Rather, it focused its search on those e-mails to which his direct supervisor had access. In response to a question from the Privacy Commissioner as to its process, Bell Canada described it as follows:

> Ms. Kelly Rose, Mr. Johnson's supervisor at the time, was instructed by an IT specialist from CGI regarding how to use the Advanced Find function. She used this function to search through all messages to find those concerning Peter Johnson for the period of time from when she became his manger on September 1st, 2004 to the date that the access was requested. The previous manager retired from the Company and there was no way to retrieve messages for this earlier period. The messages identified during the search were printed and reviewed.

[5] On May 25, 2005, prior to receiving the disclosed e-mail messages, Mr. Johnson filed a complaint with the Office of the Privacy Commissioner of Canada. His complaint, as described by the Privacy Commissioner, was that "Bell Canada had not provided him with copies of all e-mails, dating back two years, pertaining to him". Although he subsequently acknowledged that he had received some e-mail messages from Bell Canada, it was Mr. Johnson's position that those e-mails did not constitute all of the requested e-mails.

[6] In the course of the Privacy Commissioner's investigation, Bell Canada provided details of its document retention policies and practices. It was the position of Bell Canada that some of the e-mails Mr. Johnson was seeking could not be provided to him as they had been destroyed in accordance with Bell Canada's document retention policies because they served no business purpose. Specifically, there were e-mails that had been in the possession of Mr. Johnson's previous

immediate supervisor during part of the period covered by the access request (May 12, 2003 to September 1, 2004) and which had long since been deleted from the Bell Canada computer system.

[7] On June 15, 2007, the Privacy Commissioner issued her report concerning Mr. Johnson's complaint; it contained two conclusions. First, she concluded that Bell Canada had breached section 8(4)(a) of PIPEDA when it extended the time for response by a further 30 days without providing a reason for doing so. She also found that the Act was further breached in that Bell Canada failed to advise Mr. Johnson of his right to make a complaint to the Office of the Privacy Commissioner with respect to this extension. The report observed, however, that given the nature of the access request, the extension of time did seem to be reasonable in the circumstances.

[8] Secondly, she found that Bell Canada had provided Mr. Johnson with close to 600 pages of information, including that which had initially been excluded but which the Privacy Commissioner advised should be released to Mr. Johnson in redacted format. She found that Bell Canada had "now met its obligation under Principle 4.9" of PIPEDA and concluded that "Mr. Johnson's denial of access complaint is resolved".

[9] The complaint, however, had not been resolved to Mr. Johnson's satisfaction. Accordingly, he filed an application under subsection 14(1) of PIPEDA, which provides that a complainant may, after receiving a report from the Privacy Commissioner as a result of a complaint filed under PIPEDA, apply to Federal Court for a hearing in respect of any matter brought up in the complaint. As will be noted, the potential scope of a proceeding under subsection 14(1) is quite wide.

[10] The Commission appears to have taken a more narrow view of Mr. Johnson's complaint than he. Under the heading "Other" which follows the conclusion that the complaint is resolved, is a recital of facts that are material to many of the issues now before this Court. It is worth setting out this portion of the report in its entirety:

> 14. Mr. Johnson had indicated that he believed e-mails had been sent between his co-workers, and between his previous supervisor and the one in place when he made his request. On the first matter, Bell had taken the position that exchanges between employees are not part of business operations and are not included in the employee's personal file. The company stated that it did not consider this information to have been collected in the course of its business operations, and that therefore Mr. Johnson was not entitled to have access to such e-mail.
>
> 15. According to the company's internet Policy, it is acceptable for employees using company-provided internet access to have "reasonable levels of personal communication, whether by telephone or e-mail...as long as they comply with this policy." Employees are also reminded that e-mail messages must comply with the company's Code of Business Conduct.
>
> 16. Approximately 30 days worth of data can be saved before an employee has to either save the data to the hard drive or copy it to a laptop or delete it. Magnetic tapes of this data are stored off site in Toronto by a third-party service provider. After 50 days the tapes are overwritten.
>
> 17. As for e-mail between supervisors, when a supervisor leaves the company, the e-mail account is disabled after 30 days and the data is wiped out before the computer is set up for a new user. There is no company policy stipulating what employees information should be passed on to a new supervisor when an employee is transferred to another work group. The supervisor exercises his or her discretion as to what employee information is passed on. Had information been communicated between Mr. Johnson's supervisors, it would have been provided to him.

> 18. Under paragraph 4(1)(a), Part I of the *Act* applies to every organization in respect of personal information that is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.
>
> 19. While Bell took the position that personal e-mail between employees was not accessible under the *Act*, I would argue that it is. As this Office has stated in a previous case, paragraph 4(2)(b) is not intended to absolve an organization of responsibility for an employee who uses their position within the organization to collect, use or disclose personal information for their own purposes. Therefore, personal e-mail *may be* subject to the *Act* (if it contains personal information), and therefore accessible. In this instance, given the retention periods involved, there are no longer any personal e-mails between employees to search.
>
> 20. I have raised this matter as I believe it is important for Bell and its employees to be aware that personal e-mails may be considered personal information and are subject to the *Act*.

[11] In an affidavit filed in this proceeding, Mr. Johnson sets out the basis of his belief that Bell Canada failed to disclose what he described as "many" e-mail messages. The relevant portion of the affidavit reads as follows:

> 11. I believe that many e-mail messages that contain my personal information were withheld from me. The basis for my belief is as follows:
>
> a. In connection with a relatively recent police investigation, I provided the police with a statement that contained very sensitive personal information. I understand that one of the investigating officers is the spouse of Mrs. Andrea Tubrett, a Bell manager.
>
> b. Immediately after making my request to my manager, Ms. Rose, for access to my personal information under PIPEDA, I personally observed Ms. Rose speak with Ms. Tubrett. In this (*sic*) course of this conversation, both Ms. Rose and Ms. Tubrett openly cried.

> c. The finding of the Privacy Commissioner concludes that e-mail messages referring to me between employees had not been provided to me by Bell nor had they been provided to the Commissioner for her review.

[12] Mr. Johnson's principal issue, as set out in his affidavit, is that he has not been provided with access to the e-mail messages between Bell Canada employees, some of whom occupy supervisory positions, that refer to him. His complaint has three facets: (1) that Bell Canada carried out an inadequate search in response to his access request; (2) that Bell Canada has denied him access to the personal e-mails concerning him that were sent between Bell Canada employees; and (3) that Bell Canada has deleted the personal e-mails in breach of PIPEDA.

[13] Mr. Johnson in this application seeks an order under section 16(a) of PIPEDA that Bell Canada provide him with all of his personal information including all e-mail messages referring to him, damages under section 16(c) of PIPEDA as may be proven, and his costs.

ISSUES

[14] The Applicant viewed the issue before the Court to be as follows:

> [W]hether the Respondent fulfilled its obligations under Clause 4.9 of Schedule I to PIPEDA and section 8 of PIPEDA by not providing the Applicant with access to all the personal information requested and whether the Respondent violated PIPEDA by failing to live up to its obligation under section 8(8), which requires an organization to retain personal information until a requestor has exhausted his or her recourse under Part I of PIPEDA.

Bell Canada viewed the issue before the Court to be as follows:

> [W]hether the Respondent did in fact abide by the provisions of PIPEDA in making full disclosure to the Applicant of all documents found by the Respondent pursuant to the Request of May 12, 2005, while severing from some of the requested documents, information which could reveal the personal information of a third party as required by subsection 9(1) of PIPEDA.

[15] In my view, neither statement aptly captures the issues before this Court as set out in the parties' memoranda of argument and as they were developed during counsels' oral submissions. As has been held by the Federal Court of Appeal in *Englander v. Telus Communications Inc.*, [2005] 2 F.C.R. 572, the issue in a proceeding under subsection 14(1) of PIPEDA "is not the Commissioner's report, but the conduct of the party against whom the complaint is filed". Thus, the broad issue here is whether Bell Canada, in responding to Mr. Johnson's request dated May 12, 2005, complied with the requirements of PIPEDA. With respect to the conduct of Bell Canada, as noted, Mr. Johnson has raised three distinct concerns: the adequacy of the search it conducted, its alleged failure to disclose personal e-mails, and its alleged destruction of e-mails.

[16] The area of Mr. Johnson's concern, and the focus of this application, are the e-mails he alleges were sent to and from Bell Canada employees concerning him and which, from the perspective of Bell Canada, serve no business purpose. I shall refer to e-mail messages of this type as "personal" e-mails; whereas e-mail messages concerning Mr. Johnson that Bell Canada views as having a business purpose, I shall refer to as "business" e-mails.

[17] Mr. Johnson submits that the personal e-mails contain his personal information and are subject to PIPEDA; accordingly, he submits that the focused search Bell Canada conducted was inadequate to meet its responsibilities under the Act, and that Bell Canada breached the Act in deleting these e-mails while his request was underway.

[18] The questions the Court must deal with are as follows:

1. Are personal e-mails subject to PIPEDA and disclosure by Bell Canada in response to Mr. Johnson's access request?
2. Did Bell Canada conduct a search that met its obligations under PIPEDA in response to Mr. Johnson's access request?
3. Did Bell Canada fail to preserve personal information that would have been responsive to the access request, in breach of PIPEDA?
4. If there was a violation of Mr. Johnson's rights under PIPEDA, what remedies are available to him and, what remedies ought this Court grant?

ANALYSIS

Is this matter moot?

[19] The Privacy Commissioner found, in paragraph 19 of the report cited above, that "given the retention periods involved, there are no longer any personal e-mails between employees to search". Bell Canada submitted that given that the issues in this application revolve around these non-existent personal e-mails, this application is moot and should not be dealt with by the Court. I am not convinced that the Privacy Commissioner was correct in concluding that there are no longer any

personal e-mails between employees to search. E-mail messages may be saved on hard drives and other storage media, as was the case with those e-mails Bell Canada did produce from Mr. Johnson's supervisor. When saved in this manner, they are not subject to deletion from Bell Canada's server and back-up systems in accordance with its retention policy. Mr. Johnson specifically mentions the possible e-mails received or sent by a Bell Canada manager other than his immediate supervisor. That person had no supervisory responsibilities with regards to Mr. Johnson and the record indicates that Bell Canada made no inquiries of her as to whether she had saved any e-mails that referenced Mr. Johnson. If the Applicant's submission on the application of PIPEDA to personal e-mails is accepted, it may be that Bell Canada's search was inadequate and a more thorough search may reveal additional e-mails that have not yet been produced. Accordingly, I am not convinced, on the record before me, that this application is moot.

What is the nature of this proceeding?

[20] The legislative scheme under PIPEDA is atypical from an administrative law standpoint, not least because the Privacy Commissioner's recommendations are non-binding. Deference to an administrative decision-maker is therefore not possible, in that there is no real decision of which to speak. This has implications for the Court's role, as it was pointed out by Justice Décary in *Englander*: "[T]he hearing is a proceeding *de novo* akin to an action and the report of the Commissioner, if put into evidence, may be challenged or contradicted like any other document adduced in evidence." The evidence in this application is found in the report of the Privacy Commissioner and the affidavits filed by Mr. Johnson and by Simeon Doucette, Human Rights and Privacy Coordinator for Bell Canada.

[21] The Federal Court of Appeal in *Englander* reviewed the history leading to the passage of PIPEDA and found that PIPEDA is a compromise both as to substance and as to form. In substance, it is a compromise between the commercial interests of business and the privacy rights of individuals. In form, it is a compromise or, more accurately, an amalgam of the legal and non-legal. While Part I of the Act is drafted in the usual manner of legislation, Schedule I, which was borrowed from the CSA Standard, is notably not drafted following any legislative convention. As a result, the Court of Appeal in *Englander* has directed that construction of this legislation should be guided by "flexibility, common sense and pragmatism". With this in mind, I turn to consider the questions previously posed.

Are Personal E-mails Covered By PIPEDA?

[22] There appears to be no question that if an e-mail concerning an individual employee is sent by one employee to another in the course of the employer's business, or if the employer receives an e-mail from a third party concerning an employee and that information is used by the employer in its business operations, for example, in the performance appraisal of the employee, those e-mails are accessible by the employee under PIPEDA. In fact, the e-mails produced by Bell Canada in response to Mr. Johnson's request apparently fell within this characterization. In response to a question from the Privacy Commissioner as to Bell Canada's position regarding Mr. Johnson's entitlement to access exchanges of e-mails that contain personal information about him, Bell Canada responded:

> Exchanges of e-mail between colleagues may serve a business purpose or be for personal reasons. Certainly, we as employer have

> some (limited) ability to view personal messages, however when there is no business content in the messages and therefore no business reason for using the information, we cannot use the information for any purpose and must preserve its confidentiality. The exchanges of a personal nature between colleagues of an employee are not part of business operations and are not included in the employee's personal file. We do not consider this information to have been collected in the course of our business operations. As a result we do not believe that Mr. Johnson is entitled to have access to such e-mail.

[23] Mr. Johnson submits that as personal e-mails contain his personal information he has a right to access them under clause 4.9 of Schedule I to PIPEDA, the relevant provisions of which are as follows:

4.9 Principle 9 - Individual Access	4.9 Neuvième principe — Accès aux renseignements personnels
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.	Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.
Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include	Note : Dans certains cas, il peut être impossible à une organisation de communiquer tous les renseignements personnels qu'elle possède au sujet d'une personne. Les exceptions aux exigences en matière d'accès aux renseignements personnels devraient être restreintes et

information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

précises. On devrait informer la personne, sur demande, des raisons pour lesquelles on lui refuse l'accès aux renseignements. Ces raisons peuvent comprendre le coût exorbitant de la fourniture de l'information, le fait que les renseignements personnels contiennent des détails sur d'autres personnes, l'existence de raisons d'ordre juridique, de raisons de sécurité ou de raisons d'ordre commercial exclusives et le fait que les renseignements sont protégés par le secret professionnel ou dans le cours d'une procédure de nature judiciaire.

4.9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.1 Une organisation doit informer la personne qui en fait la demande du fait qu'elle possède des renseignements personnels à son sujet, le cas échéant. Les organisations sont invitées à indiquer la source des renseignements. L'organisation doit permettre à la personne concernée de consulter ces renseignements. Dans le cas de renseignements médicaux sensibles, l'organisation peut préférer que ces renseignements soient communiqués par un médecin. En outre, l'organisation doit informer la personne concernée de l'usage qu'elle fait ou a fait des renseignements et des tiers à qui ils ont été communiqués.

[24] Mr. Johnson submits that the only circumstances under which Bell Canada may deny him access to his personal information in those personal e-mails are those specific exceptions set out in subsection 9(3) of PIPEDA, as follows:

9(3) Despite the note that accompanies clause 4.9 of Schedule 1, an organization is not required to give access to personal information only if	9(3) Malgré la note afférente à l'article 4.9 de l'annexe 1, l'organisation n'est pas tenue de communiquer à l'intéressé des renseignements personnels dans les cas suivants seulement :
(a) the information is protected by solicitor-client privilege;	*a*) les renseignements sont protégés par le secret professionnel liant l'avocat à son client;
(b) to do so would reveal confidential commercial information;	*b*) la communication révélerait des renseignements commerciaux confidentiels;
(c) to do so could reasonably be expected to threaten the life or security of another individual;	*c*) elle risquerait vraisemblablement de nuire à la vie ou la sécurité d'un autre individu;
(c.1) the information was collected under paragraph 7(1)(b);	*c*.1) les renseignements ont été recueillis au titre de l'alinéa 7(1)*b*);
(d) the information was generated in the course of a formal dispute resolution process; or	*d*) les renseignements ont été fournis uniquement à l'occasion d'un règlement officiel des différends;
(e) the information was created for the purpose of making a disclosure under the Public Servants Disclosure Protection	*e*) les renseignements ont été créés en vue de faire une divulgation au titre de la *Loi sur la protection des fonctionnaires*

Act or in the course of an investigation into a disclosure under that Act.	*divulgateurs d'actes répréhensibles* ou dans le cadre d'une enquête menée sur une divulgation en vertu de cette loi.
However, in the circumstances described in paragraph (b) or (c), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from the record containing any other information for which access is requested, the organization shall give the individual access after severing.	Toutefois, dans les cas visés aux alinéas *b*) ou *c*), si les renseignements commerciaux confidentiels ou les renseignements dont la communication risquerait vraisemblablement de nuire à la vie ou la sécurité d'un autre individu peuvent être retranchés du document en cause, l'organisation est tenue de faire la communication en retranchant ces renseignements.

[25] In *Wansink v. TELUS Communications Inc*., [2007] 4 F.C.R. 368 (C.A.), the Court of Appeal held, with reference to subsection 7(1) of PIPEDA, that "the very fact that Parliament has expressly asked that the note in Schedule I be ignored is a significant indication if its desire to limit the circumstances in which consent to collection of personal information is not required to those it describes in subsection 7(1)". In my view, the same is true of section 9(3) of PIPEDA. If PIPEDA otherwise applies to the information, then the only circumstances when access may be refused are those set out in section 9(3) of PIPEDA.

[26] As noted previously, Bell Canada takes the position that personal e-mails do not fall under PIPEDA. In its Memorandum of Argument, Bell Canada writes:

> …'personal e-mails' between colleagues, which are not collected, used or disclosed in connection with the operation of a federal business within the meaning of section 4(1) of PIPEDA are not covered by PIPEDA and are therefore not subject to the individual right of access. Rather, they constitute personal information about a third party to which an individual cannot be granted access pursuant to subsection 9(1) of PIPEDA. (emphasis in original)

[27] The relevant exceptions to the application of PIPEDA are set out in section 4 of PIPEDA, which reads as follows:

4.(1) This Part applies to every organization in respect of personal information that	4. (1) La présente partie s'applique à toute organisation à l'égard des renseignements personnels :
(a) the organization collects, uses or discloses in the course of commercial activities; or	*a*) soit qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales;
(b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.	*b*) soit qui concernent un de ses employés et qu'elle recueille, utilise ou communique dans le cadre d'une entreprise fédérale.
(2) This Part does not apply to	(2) La présente partie ne s'applique pas :
(a) any government institution to which the Privacy Act applies;	*a*) aux institutions fédérales auxquelles s'applique la *Loi sur la protection des renseignements personnels*;
(b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or	*b*) à un individu à l'égard des renseignements personnels qu'il recueille, utilise ou communique à des fins personnelles ou domestiques et à aucune autre fin;

(c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.	*c*) à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique à des fins journalistiques, artistiques ou littéraires et à aucune autre fin.
(3) Every provision of this Part applies despite any provision, enacted after this subsection comes into force, of any other Act of Parliament, unless the other Act expressly declares that that provision operates despite the provision of this Part.	(3) Toute disposition de la présente partie s'applique malgré toute disposition — édictée après l'entrée en vigueur du présent paragraphe — d'une autre loi fédérale, sauf dérogation expresse de la disposition de l'autre loi.

[28] Mr. Johnson submits that the personal e-mails fall within the description set out in subsection 4(1)(b) because they are personal information about him, an employee of Bell Canada, and they are collected, used or disclosed by Bell Canada in connection with the operation of a federal work, undertaking or business.

[29] Mr. Johnson submits, and I agree, that an electronic message about or concerning him meets the definition of "personal information" in subsection 2(1) of PIPEDA which reads as follows:

"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.	«renseignement personnel » Tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail.

[30] As was noted by the Federal Court of Appeal in *Rousseau v. Canada (Privacy Commissioner)*, 2008 FCA 39, the definition of personal information as meaning "information about an identifiable individual" entails that the Act is very far reaching. In *Rousseau* it was held that the handwritten notes of a doctor, taken during an independent medical examination of an insured person by a doctor at the request of the insurance company, were personal information under PIPEDA. In my view, there can be question that e-mail messages concerning a person constitute personal information of that person under PIPEDA. Further, there is no dispute that the e-mails that Mr. Johnson was seeking concerned him at a time when he was an employee of Bell Canada. The real issue is whether these e-mails were collected, used or disclosed by Bell Canada in connection with the operation of a federal work, undertaking or business. More specifically, it is whether Bell Canada collected these e-mails, as there is no evidence of use or disclosure.

[31] It is a reality of our electronic world that computer systems store the data transmitted on them. E-mail messages are stored, at least for some period of time, in the sender's "sent" box and the recipient's "in" box. Even when deleted, they reside in the "deleted" items box for a period of time. Further, the data are stored on the servers through which they travel during transmission and the information on those servers and on the individual computers used to transmit the e-mail messages is captured and backed-up on a regular and periodic basis. Organizations put systems and procedures in place deliberately to capture such information as is relevant to the organization and its business needs. The reality is that non-relevant information is also captured. Just as the cod fisherman's nets will capture whiting, flounder, hake, squid, butterfish, or other species in addition

to the cod which is the fisherman's target, the organization's data storage system which is intended to capture business e-mail will capture personal e-mails, jokes, spam, family pictures and other non-business data transmitted on the system.

[32] As noted previously there is an exception from the application of the Act in subsection 4(2)(b) for personal information collected by an individual solely for the individual's personal reasons. If this information, exempt in the hands of the individual, is an e-mail sent or received at work, it would be contrary to the purposes of the Act if that same information, once stored on the organization's back-up system, would then not also be exempt from production by the organization. To find otherwise would not accord with common sense and pragmatism and, in my view, would require an interpretation of the Act that would not have been contemplated by its legislators.

[33] However, subsection 4(2)(b) applies only to exempt individuals from PIPEDA, not corporations or other business entities. The only exemption applicable to business entities is subsection 4(2)(c), which deals only with information collected for journalistic, artistic or literary purposes and which would have no application to e-mail information of the sort under discussion. Accordingly, the exemption must be found in the scope clause of the Act – in subsection 4(1) which I set out again for ease of reference:

4.(1) This Part applies to every organization in respect of personal information that	4.(1) La présente partie s'applique à toute organisation à l'égard des renseignements personnels :
(a) the organization collects, uses or discloses <u>in the course of commercial activities</u>; or	*a*) soit qu'elle recueille, utilise ou communique <u>dans le cadre d'activités commerciales</u>;

(b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business. (emphasis added)	*b*) soit qui concernent un de ses employés et qu'elle recueille, utilise ou communique dans le cadre d'une entreprise fédérale.

The emphasized phrases must have some meaning. If it was intended that everything "collected" by the employer organization was subject to disclosure under PIPEDA, the phrases emphasized would be redundant. In my view, these phrases are to be interpreted with reference to the business realities of the commercial world and the organization. It is only that information that the organization collects because it has a commercial need for it that is captured by PIPEDA in subsection 4(1).

[34] The Federal Court of Appeal in *Englander* noted that the focus of PIPEDA was the commercial world:

> [PIPEDA] is undoubtedly directed at the protection of an individual's privacy; but it is also directed at the collection, use and disclosure of personal information by commercial organizations. It seeks to ensure that such collection, use and disclosure are made in a manner that reconciles, to the best possible extent, an individual's privacy with the needs of the organization. There are, therefore, two competing interests within the purpose of the PIPED Act: an individual's right to privacy on the one hand, and the commercial need for access to personal information on the other. However, there is also an express recognition, by the use of the words "reasonable purpose," "appropriate" and "in the circumstances" (repeated in subsection 5(3)), that the right of privacy is not absolute. (emphasis added)

[35] The Applicant submits that these personal e-mails, this bycatch of the computer systems and back-up systems in place to capture and save information for which the organization has a

commercial need, fall within the meaning of subsection 4(1)(b) as "it is information that is being handled 'in connection with' (or 'dans le cadre de') the operation of the Respondent's business". First, in my view, the information is not being "handled" by Bell Canada. Like the bycatch of the cod fisherman, personal e-mail is the bycatch of the commercially valuable information that is being handled by Bell Canada. Secondly, to be information collected in connection with the operation of the business, requires that there be a business purpose for the information. There is none with respect to personal e-mails. In fact, from the viewpoint of organizations like Bell Canada, personal e-mails are refuse that take up valuable space and time. It is for this reason, among others, that organizations discourage or limit employee utilization of their computer systems for personal reasons.

[36] Mr. Johnson further submits that while the e-mails may not have a business purpose, from Bell Canada's viewpoint, this alone does not exempt them from PIPEDA. He points out that the information was transmitted using Bell Canada's business systems and, focusing on e-mails transmitted among those employees above him in the organizational hierarchy, he submits that "the supervisors may have had personal reasons to transmit such information, but it was only done by virtue of their employment with the Respondent and the supervisory position vis-à-vis the Applicant".

[37] The Applicant in this characterization is attempting to remove the personal e-mails in issue from the exemption provided in subsection 4(2)(b) of personal information that an individual collects for personal reasons. The Privacy Commissioner in her report references a previous case in

which she found that subsection 4(2)(b) "is not intended to absolve an organization of responsibility for an employee who uses their position within the organization to collect, use or disclose personal information for their own purposes". This is a reference to PIPEDA Case Summary #346.

[38] In Case Summary #346 the vice-president of a company sent an interoffice e-mail with the complainant's name in the subject line and with a message that asked: 'Does anyone know what firm he is with?' Although the vice-president stated that his reason for sending the message was business-related, the Privacy Commissioner did not believe him and agreed with the complainant that he likely had a personal reason for sending the e-mail. The Privacy Commissioner found that there was no breach of PIPEDA as there had been no evidence that the complainant's personal information had been collected – there was only an attempt to collect it. The Privacy Commissioner found that the vice-president sent the e-mail in his capacity as vice-president of the company, using the company's e-mail system and office equipment. She reasoned that while he may have had personal reasons for sending the e-mail, he did not act as an individual in so doing, and she found that his actions had every appearance of being conducted on behalf of the company, for business-related reasons. That is the context in which she held, in the terms cited above, that subsection 4(2)(b) is not meant to absolve a company of responsibility for the actions of its employees.

[39] I support the Privacy Commissioner in her view that the exemption in subsection 4(2)(b) cannot be used to exclude from PIPEDA personal information that would otherwise be accessible, under the guise that it has been collected, used or disclosed for personal reasons. However, in my

view, the exemption in subsection 4(2)(b) is available to personal information that an individual collects, uses or discloses solely for personal or domestic purposes, and this exemption is not forfeit simply because the individual uses equipment available by virtue of his or her employment or position. To hold otherwise would strip subsection 4(2)(b) of any meaning, as virtually any use of the employer's computer systems would result in the loss of the subsection 4(2)(b) exemption and bring within the ambit of PIPEDA personal information that has no value or use to the commercial organization. Thus, while there may conceivably be instances when the subsection 4(2)(b) protection will be lost, those will be exceptional circumstances resulting from unique fact situations. There is no evidence before the Court that such exceptional circumstances exist here.

[40] Accordingly, the answer to the first question: 'Are personal e-mails subject to PIPEDA and disclosure by Bell Canada in response to Mr. Johnson's access request?', is No.

Did Bell Canada conduct a sufficient search in response to the request?

[41] I am of the opinion that an organization, when searching for information in response to a request stated as broadly as Mr. Johnson stated his, is not required to assume that information otherwise exempt from PIPEDA by virtue of subsection 4(2)(b) may have lost that status. Absent some reason to believe that there were personal e-mails that through some exceptional circumstance lost the exemption and fell under PIPEDA, Bell Canada was not required to conduct a broad search for information in response to the request.

[42] The search it was required to conduct was a search that could reasonably be expected to produce the personal information of Mr. Johnson that, in the ordinary course, would fall under PIPEDA. In my view that is exactly what Bell Canada did in this case. From the viewpoint of its business operations it reasonably expected that the e-mail information concerning Mr. Johnson would be in the hands of his direct supervisor. There is no evidence that there would be any other business e-mails concerning Mr. Johnson in the control of any other employee of Bell Canada.

[43] Further, there is insufficient evidence to suggest that any of the personal e-mails Mr. Johnson seeks to access have lost the exemption in subsection 4(2)(b). Where the organization has conducted a reasonable search in response to an access request, if the party who made the request claims that there is other information that has not been produced, the burden must lie on the requester to establish at least a *prima facie* case that the search has been inadequate. The statement in paragraph 11 of Mr. Johnson's affidavit, quoted previously, does not come close to establishing that there may be other information in the possession of Bell Canada that has not been produced.

[44] Bell Canada submitted that there is an obligation on the part Mr. Johnson, as the person requesting access to his personal information, to cooperate by specifying where Bell Canada ought to search and that "the Applicant must, at the very least, provide objective, useful criteria aimed at narrowing the scope of the required search". In support of this position Bell Canada relies on Principle 4.9.2 of Schedule I of PIPEDA which provides that "an individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use,

and disclosure of personal information". It also relies of the decision of the Québec Commission d'accés à l'information in *Deschênes v. Banque C.I.B.C.*, [2003] C.A.I. 249.

[45] The position of the Québec Commission d'accés à l'information in *Deschênes* as to the responsibilities of the parties involved in that case is similar to that I have taken here. Ms. Deschênes had been an employee and a customer of the Bank. She requested notes from her mortgage file as well as any communication between the Toronto and Montréal offices with respect to her dismissal and late payments. The Bank produced the result of what it viewed as a reasonable search for these records. Ms. Deschênes was of the view that there were other records that had not been produced. The Commission, in dismissing Ms. Deschênes' complaint, accepted that the search conducted by the Bank was reasonable and that Ms. Deschênes had the burden to establish that there were documents that had not been produced. The relevant portion of the decision reads as follows:

> [78] Mr. Deschênes provided precise and uncontradicted testimony establishing that after one year the Bank reused the recordings which could have contained e-mail bearing Ms. Deschênes' name. In light of this evidence, the Commission finds that the Bank no longer has other e-mails.
>
> [79] The Bank called Mr. Deschênes, Mr. Paiement and Ms. Condrain to testify before the Commission. The Bank also filed the supplemental affidavits of Ms. Condrain, Ms. Boivin, and Ms. Levine. All of them declared under oath that, after a careful search, the Bank did not possess any documents other than those already given to Ms. Deschênes or any documents still at issue.
>
> [80] In a matter such as the one under review, it is reasonable that Ms. Deschênes, in submitting a request for access to all information held by the Bank concerning her as a client and former employee, would collaborate in identifying the documents sought.

> [81] It was in the context of this endeavour that the Commission sought the collaboration of the Bank's representatives to undertake an additional search. Indeed, this effort was not in vain, as some documents were found.
>
> [82] This last step completed, the onus is on Ms. Deschênes to adduce concrete evidence constituting a commencement of proof with respect to the existence of any document containing personal information about her, as defined in article 2 of the Act. The Commission is of the opinion that the last letters received from Ms. Deschênes do not refer to a concrete situation that would suggest that other documents existed.
> (The Court's translation)

[46] I am of the view that the position stated by Bell Canada that Mr. Johnson "had a responsibility to focus his request" overstates the responsibility of an applicant making an access request. In my view, and in keeping with the practicality of the application of PIPEDA to a request that may suggest an extensive, costly and time-consuming search, the organization receiving a broad request such as that made by Mr. Johnson has two options open to it: (1) it can inquire of the party making the request if he can be more specific as to the information he is requesting, in which case the requesting party does have an obligation to cooperate in defining his request, or (2) it can conduct a reasonable search of information that it can reasonably expect to be responsive to the request. In this case Bell Canada chose the latter course.

[47] Where that latter course is chosen, absent further evidence, one need not assume that there is any reason to conduct a search for messages that fall outside the scope of those which the organization reasonably believes that it would collect, use and disclose in the course of its business operations.

[48] Accordingly, the answer to the second question: 'Did Bell Canada conduct a search that met its obligations under PIPEDA in response to Mr. Johnson's access request?', is Yes.

Did Bell Canada destroy information contrary to PIPEDA?

[49] Bell Canada had an obligation under subsection 8(8) of PIPEDA to retain and preserve Mr. Johnson's personal information until all recourse available to him, including the present application, was exhausted.

8. (8) Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have.	8. (8) Malgré l'article 4.5 de l'annexe 1, l'organisation qui détient un renseignement faisant l'objet d'une demande doit le conserver le temps nécessaire pour permettre au demandeur d'épuiser ses recours.

[50] First, there is no evidence that there were any e-mails subject to disclosure under PIPEDA that were not delivered to Mr. Johnson or retained by Bell Canada. Secondly, given the nature of Bell Canada's retention policy, which is typical in the corporate world, it is perhaps inevitable that some business e-mails may have been deleted in the time taken to process the access request. The Bell Canada policy provides that data on a laptop is retained only for 30 days and, if not saved by the employee, is automatically deleted. That data is also backed-up on tapes but those tapes are overwritten after 50 days. As a result, this electronic information is not in a static state. It is a river of information flowing towards an abyss, and each day a portion of that information is lost.

[51] It cannot be seriously suggested that an organization has a responsibility to recover deleted or overwritten data in the absence of compelling evidence that it existed and that it can be recovered at a reasonable cost. Further, in my view, such a Herculean task should only be required to be undertaken, if ever, in circumstances where there is a critical need for the recovered information. In this respect, I concur with the view expressed by the Québec Commission d'accés à l'information in *Labreque c. Québec*, [2005] C.A.I. 221, where it stated:

> [25] The Commission is of the opinion that in principle, one shouldn't require an access coordinator to locate, restore, and reproduce electronic documents of this type (e-mails) which have been destroyed, or overwritten by new versions, or which are stored in backup files.
>
> [26] Considering the relatively short time frame that an access coordinator has in which to respond to an access request under the Act (30 days maximum), and considering the technical complexity of restoring an electronic document such as an e-mail - a complexity which is familiar to the Commission on account of its expertise - the Commission is of the opinion that such an undertaking raises serious practical difficulties.
>
> [27] It is within the specialized knowledge of the Commission that retrieval operations of e-mails which have been destroyed, overwritten, or stored in backup files, may involve unforeseen and sometimes major expenses, which could, in some instances, be charged to the person requesting access.
> (The Court's translation)

[52] It is impractical to require a company like Bell Canada to stop its corporate retention policies each time an access request is made; especially as it is not known if any of the information that would otherwise be lost into the abyss is even responsive to the request. From a practical and pragmatic standpoint, what subsection 8(8) of PIPEDA requires of an organization is that it retain

that information that it has discovered in its search that is or may be responsive to the request, until the person making the request has exhausted all avenues of appeal. As I have indicated, there is no evidence that Bell Canada did not do so in this case.

[53] Accordingly, the answer to the third question: 'Did Bell Canada fail to preserve personal information that would have been responsive to the access request, in breach of PIPEDA?', is No.

Remedies

[54] Having found that there has been no violation of PIPEDA by Bell Canada, it is unnecessary to consider the remedies that would have been available had there been a violation on its part. Accordingly the fourth question need not be answered.

JUDGMENT

THIS COURT ORDERS AND ADJUDGES that this application for judicial review is dismissed with costs.

"Russel W. Zinn"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-1385-07
STYLE OF CAUSE:	DONALD PETER JOHNSON v. BELL CANADA
PLACE OF HEARING:	Halifax, Nova Scotia
DATE OF HEARING:	August 21, 2008
REASONS FOR JUDGMENT AND JUDGMENT:	ZINN J.
DATED:	September 26, 2008

APPEARANCES:

David T. S. Fraser	FOR THE APPLICANT
Maryse Tremblay	FOR THE RESPONDENT

SOLICITORS OF RECORD:

McInnes Cooper Barristers and Solicitors Halifax, Nova Scotia	FOR THE APPLICANT
Heenan Blaikie LLP Barristers and Solicitors Montreal, Quebec	FOR THE RESPONDENT