Federal Court Cour fédérale

Date: 20180522

Docket: T-1424-16

Citation: 2018 FC 525

Ottawa, Ontario, May 22, 2018

PRESENT: The Honourable Mr. Justice Roy

BETWEEN:

ANGELA MIGLIALO

Applicant

and

ROYAL BANK OF CANADA

Respondent

JUDGMENT AND REASONS

I. Introduction

[1] Ms. Angela Miglialo, the applicant, brings an application pursuant to section 14 of the *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5) [PIPEDA].

[2] The applicant claims damages in the order of $100,000.00 to $250,000.00 (depending on the notice of application or the memorandum of fact and law) for an unauthorized access to her

account at the Royal Bank of Canada [RBC] and the disclosure of financial information. It is not a matter of dispute that there was an unauthorized access to the applicant's account by a RBC employee. So much was acknowledged by RBC upon discovering the breach in April 2013. That is also the conclusion reached by the Privacy Commissioner [or the Commissioner] in the Report of Findings [or the Report] of October 21, 2015.

[3] The applicant suggests that the person accessing without authorization her account disclosed the information afterwards. The Privacy Commissioner found that there was insufficient evidence in order to reach that conclusion.

[4] It seems that the central issue in this application is whether damages are owed by RBC, either for the unauthorized use, or the use and disclosure, of private information, and, if so, what would be an appropriate amount, if any, in the circumstances.

II. Facts

A. Background

[5] The applicant, who lives in Calgary and does her banking at RBC, was suspecting for some time in 2011, 2012 and early 2013 that information about her accounts with RBC was being made available without her authorization. The initial concerns which first led to the applicant's suspicion that her RBC investment accounts' private information had been disclosed arose in 2011 and continued into 2012. The applicant's mother resides in Montreal and they kept in touch through regular telephone conversations. The applicant's mother apparently started

asking the applicant about the beneficiaries on the applicant's investment accounts. In particular, the applicant's mother would have discussed her financial plans following her death and asked the applicant whether they would be keeping their money together. The conversations became increasingly uncomfortable for the applicant and she decided to put a temporary end to their calls in late 2012.

[6] On September 4, 2012, the applicant decided to reach out to her RBC Branch Manager in Calgary about her suspicion that the privacy of her RBC investment accounts had been breached. At the hearing of this case, the applicant testified that she was particularly concerned that the identity of the beneficiaries would be revealed to her family. The applicant told the manager she suspected that the breach had been perpetrated by her brother's girlfriend who worked at RBC in Montreal [the RBC employee]. However, the information about the RBC employee was rather sketchy, to the point where an investigation would not be conducted.

[7] On January 25, 2013, the applicant met with RBC and signed a consent to have the names of the beneficiaries removed from her accounts. According to the applicant's memorandum of fact and law, she resumed her telephone calls and "noticed that my mother had ceased from asking beneficiary related questions". The fact that Ms. Miglialo's mother was not asking anymore uncomfortable questions about her accounts led her to believe that she had her accounts' information. There is no indication as to the content of these accounts and, thus, the Court is unable to ascertain the sensitivity and value of the confidential information. It seems that after January 25, although the identity of beneficiaries had been removed, there would be left at least information about the amounts in the accounts.

[8] Ms. Miglialo was able to give more precise information on March 18, 2013, about the person she suspected of having gained access to her accounts' information such that the Corporate Investigation Department of RBC was able to run a security check for years 2010, 2011 and 2012. On April 12, 2013, an investigator of RBC contacted the applicant to discuss her complaint. The investigation at that stage did not reveal any unauthorized access by the person suspected by the applicant, or anyone else, during 2010, 2011 and 2012. On that occasion and in view of the unsuccessful results of the investigation at that stage, the investigator asked questions about the applicant's personal circumstances. I note that the applicant was also asked on March 18, 2013, about the reasons she had suspicions about that particular RBC employee. The applicant reports that the investigator indicated that the investigation would continue.

[9] RBC expanded its investigation to include a security check that would cover the first few months of 2013 after the applicant raised the issue following shortly after the April 12 conversation. On April 29, 2013, the investigator called the applicant to advise her that the investigation revealed that the RBC employee she suspected had accessed the applicant's investment accounts on one occasion in February 2013, without any apparent business reason, but that the matter had been appropriately dealt with. We now know that the reported breach occurred on February 24, 2013. This means that the breach took place after the period in which the applicant's mother was asking her overly-intrusive questions about her estate plans, as well as after the applicant decided to remove the names of her beneficiaries. There is no indication on the record before the Court that there was ever an authorized access that allowed for the beneficiaries to be identified.

[10] Prior to April 29 when an RBC investigator communicated with the applicant (April 25, 2013), another RBC investigator interviewed the RBC employee who, according to the evidence, admitted viewing the accounts of Ms. Miglialo, but denied having disclosed the information to anyone.

[11] According to the applicant's own memorandum of fact and law, the RBC investigator counselled her not to speak with her family about the unauthorized access when he disclosed it to her on April 29. Evidently, the applicant did not take the advice. Upon her return from China in June 2013, Ms. Miglialo called and confronted her mother, according to the first of a series of reports prepared by a Behavioural Health Consultant with the Alberta Health Services. According to the reports, which were filed into evidence by the applicant and adopted by her, they did not speak together for the rest of the year following the June conversation. At the hearing of the case, the applicant testified that her mother was very upset and emotional. It is difficult to accept the applicant's evidence that, although she does not dispute the use of the word "confront", she broke the news of the access to her account in a rather casual manner. The mother's reaction and the fact that they did not speak for months suggest that the encounter was robust.

[12] The fifteen reports produced by the Behavioural Health Consultant, from February 2014 to November 2015, tend to show that the applicant was affected by the strained family relationship for which she blames the privacy breach. For instance, in the July 17, 2014, report, one reads that "Angela feels like the reported breach of privacy has damaged her relationship with the family". She believes that the information was accessed and disclosed to family

members. The reports also note that Ms. Miglialo wished to pursue the matter, first before the Privacy Commissioner, and then before the Court.

B. The Report of the Office of the Privacy Commissioner

[13] Unsatisfied with the RBC investigator's response on April 29, 2013, the applicant escalated her complaint to various authorities, including within RBC. Thus, on September 24, 2013, RBC's Regional Vice-President wrote to Ms. Miglialo offering her an apology. Her contacts with the RBC's office of the Ombudsman, to receive compensation, and the RBC's Chief Privacy Officer did not generate a further remedy (January 13, 2014, and March 11, 2014). The monetary compensation she was seeking never materialized. She filed subsequently a complaint with the Privacy Commissioner who investigated the matter.

[14] On October 21, 2015, the Office of the Privacy Commissioner issued a Report of Findings respecting the applicant's complaint. The Office of the Privacy Commissioner held as follows:

> 30. Overall, we are satisfied that RBC responded to and investigated the complaint effectively and efficiently, with a view to protecting her personal information.
>
> 31. The evidence demonstrates that from the outset, RBC generally followed up on the complainant's concerns and inquiries in a timely manner. It could be said that there was a noticeable delay of several months before RBC began this internal investigation in 2013. However, the evidence demonstrates that this delay can be traced back to the complainant, on whom the onus was at that time to provide RBC with basic – and in our view highly necessary and relevant – information so that RBC's Internal Investigative section could properly identify and locate the suspected employee and reasonably justify and surreptitious probing by the employer into an employee's account access records.

32. There is no dispute that an employee of RBC accessed the complainant's personal financial information without a business reason in February 2013. RBC has consistently acknowledged the incident to the complainant ever since the conclusion of its internal investigation into the complainant's concerns. Our Office considers such access to be a use under PIPEDA. Consequently, Principle 4.5 was contravened.

33. We found no evidence to suggest that the employee in question had accessed (or sought access) to the information on any other day than the one specified by RBC in its Internal investigation report.

34. As for whether there was a subsequent disclosure of the complainant's personal financial information to unauthorized third parties (e.g. to the complainant's family members), the complainant bases this allegation solely on a perceived change in her mother's behaviour in their telephone conversations. However, our investigation revealed that in 2013 the complainant confirmed to RBC's CIS representative that her mother had never actually shared any specific information about the complainant's banking investments with her, nor had her mother ever specifically questioned the complainant's choice of beneficiaries. Thus, in the absence of more substantial evidence, our view is that there is not sufficient evidence to confirm the allegation of a disclosure occurring.

35. The safeguards aspect of this complaint comprises several PIPEDA principles.

36. We found little evidence to suggest that the bank was not safeguarding the personal information of its clients in an appropriate manner and, more specifically, is not taking into account the more sensitive nature of certain information.

37. RBC appears to have fulfilled its obligations to make its employees aware of the importance of maintaining confidentiality of personal information. The RBC employee at the center of this complaint was aware of their duty to ensure the privacy and confidentiality of the complainant's personal information; the employee simply neglected to abide by the rules. We view these actions to be an exception rather than an indication of a broader, systemic issue.

38. Lastly, we are satisfied with the corrective actions that RBC took vis-a-vis its employee at the centre of this complaint. The

> necessary disciplinary measures were implemented in accordance with a breach of RBC's Code of Conduct.
>
> 39. Accordingly, the unauthorized use allegation under Principle 4.5 is well-founded and resolved, whereas the safeguards matter is not well-founded.
>
> [My emphasis]

[15] On August 26, 2016, the applicant filed a notice of application, pursuant to s 14(1) of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 [the Act], thus commencing the Court proceedings to seek damages from RBC. The applicant is asking the Court to allow her application and order damages against the respondent in the sums of $250 000 (as per the applicant's notice of application) or $100 000 (as per the applicant's Memorandum) for damages to the applicant's health and welfare, as well as moral prejudice, pain and suffering of the applicant, and exemplary damages. There are no details about the damages other than some more information in the reports of the Behavioural Health Consultant.

III. Issues

[16] There is no question as to whether there was an improper use of the applicant's personal information by the respondent, the parties being in agreement on this point. The issues before this Court are, therefore:

(1) Did the respondent disclose the applicant's personal information?

(2) What amount of damages, if any, should be granted by the Court?

IV. Analysis

[17] The applicant is seeking significant damages for the privacy violation which, according to the notice of application, caused her distress, humiliation, anguish and emotional anxiety. Aggravated damages are owed because of "the agony and bereavement for the value of destroying a family relationship with her mother, sister, brothers, nieces, nephews, aunts, uncles and cousins" (notice of application, p 3).

[18] Ms. Miglialo brings this matter before the Court on the basis of section 14 of PIPEDA, after the Commissioner issued his Report on October 21, 2015. PIPEDA provides specifically that the Court has jurisdiction in the nature of discretion to "award damages to the complainant, including damages for any humiliation that the complainant has suffered" (para 16(c)), a jurisdiction that the Commissioner does not have. The Privacy Commissioner does not have jurisdiction to grant damages.

PIPEDA

[19] PIPEDA is a rather peculiar piece of legislation. Its purpose is nevertheless clear. It is to reconcile the right to privacy and the need for organisations to collect, use and disclose personal information at a time when technology facilitates access to information. Section 3 reads:

3 The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal	**3** La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la

information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.	communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

What makes the legislation peculiar is that it incorporates (section 5), in its Schedule 1, the Principles Set Out in the National Standards of Canada Entitled Model Code for the Protection of Personal Information. These principles constitute obligations to comply. It is not disputed that the respondent is subject to these principles. As for the principles themselves, they are not framed like regular legislation using legal drafting, but more in terms of policy or guidelines, with the force of law, where the use of the word "should" indicates a recommendation, not an obligation (subsection 5(2) of PIPEDA). PIPEDA is not an easily accessible statute, which makes the applicant's job, who is a litigant in person, even more daunting.

[20] The Federal Court of Appeal observed in *Englander v Telus Communications Inc.*, 2004 FCA 387; [2005] 2 FCR 572:

> [43] The PIPED Act is also a compromise as to form, as is amply demonstrated by the recital of its historical background. Schedule 1 is an exact replica of Part 4 of the CSA Standard adopted in 1995, which Standard in turn was based on the OECD Guidelines adopted in 1980 and to which Canada had adhered in 1984. Both the CSA Standard and the OECD Guidelines are the product of intense negotiations between competing interests, which proceeded

> on the basis of self-regulation and which did not use nor purport to use legal drafting.
>
> […]
>
> [45] The Court is sometimes left with little, if any guidance at all. Clause 4.3, for example, requires knowledge and consent "except where inappropriate." Clause 4.3.4 sets up a standard of "sensitivity of the information," only to add that "any information can be sensitive, depending on the context." Clause 4.3.5 then goes on to say that "[i]n obtaining consent, the reasonable expectations of the individual are also relevant."
>
> [46] All of this to say that, even though Part 1 and Schedule 1 of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests. Furthermore, because of its non-legal drafting, Schedule 1 does not lend itself to typical rigorous construction, In these circumstances, flexibility, common sense and pragmatism will best guide the Court.

[21] An application under section 14 of PIPEDA is not a judicial review of the Commissioner's Report, but the Report may be entered into evidence as was the case here. The scope of the application is prescribed by law. The Court is limited to the matters in respect of which the complaint about the violation of principles was made or that are referred to in the Commissioner's Report. Although the application is said to be a *de novo* action, it must be dealt with in a summary manner. The Court is engaged in a fact-finding process to determine whether the respondent violated one or more of the principles (*Randall v Nubodys Fitness Centres*, 2010 FC 681 [*Randall*]). Once a violation has been established, the Court has discretion under section 16 of PIPEDA to award damages on a principled basis that will be appropriate and just in the circumstances (*Nammo v TransUnion of Canada Inc.*, 2010 FC 1284 [*Nammo*]). The burden of proof rests on the applicant.

[22] That means in the circumstances of this case that the applicant must establish the damages suffered and that they were caused by the violation (*Biron v RBC Royal Bank*, 2012 FC 1095 [*Biron*], at para 38). Here, the applicant claims that there was an unauthorized use of her financial information and that there was disclosure of that information. As for the use, it is not contested by RBC that there was one such occurrence, on February 24, 2013. Thus, the applicant must show that there was disclosure of her information if she is to prevail on that front. It will also be for the applicant to satisfy the Court of the damages she claims she suffered as a result of the violation.

[23] The applicant not only has the burden of proof, but she must also satisfy the standard of proof which is, in all civil matters, the balance of probabilities (*F.H. v McDougall*, 2008 SCC 53; [2008] 3 SCR 41, at para 40). As the *McDougall* Court, as well as the Court in *Canada (Attorney General) v Fairmont Hotels Inc.*, 2016 SCC 56; [2016] 2 SCR 720, at para 36, found the "evidence must always be sufficiently clear, convincing and cogent". I am afraid the evidence of that quality was dearly missing in this case.

The allegations

[24] The complaint made to the Privacy Commissioner was clearly focused on the disclosure of the financial information to the applicant's family members. Thus, Ms. Maglialo was alleging not only that there had been unauthorized access to her financial information, which was never disputed, but also that there was disclosure of that information to family members. That, claimed the applicant, resulted in "irreconcilable damage with my family members" which "caused me a great deal of humiliation and embarrassment". The suggestion is that the damages suffered came

from the disclosure made by RBC, or one of its agents, to the applicant's family members. In fact, the reports of the Behavioural Health Consultant, which postdate the confrontation with the applicant's mother and the periods of many months following when they were not on speaking terms, show clearly that it is the family relationship that concerned the applicant. The applicant also complained about the manner in which RBC officials dealt with her.

[25] The parties are *ad idem* that an employee of the RBC, who was a financial advisor in Montreal, accessed the applicant's financial information without having a business reason. The case was argued by the applicant on the basis that she was the girlfriend of the applicant's brother. For privacy reasons, neither RBC nor the Privacy Commissioner identified the RBC employee. According to the uncontradicted evidence, the unauthorized access occurred on February 24, 2013, and that happened only once.

[26] The applicant contends that her suspicion about an RBC employee accessing her accounts' information came from her mother's persistent questions in 2011-2012 about beneficiaries. That, it seems, made her suspect her brother's girlfriend, whom she could not identify. The questioning led to a cessation of weekly phone calls with her mother in 2012. Once the conversations resumed in early 2012, the applicant's mother was not raising anymore the issue of beneficiaries, which made the applicant again believe that her mother knew. The evidence shows that the only access to the financial information occurred after the information about beneficiaries had been deleted (see memorandum of fact and law, p 141, where one reads that "I replied that following the meeting on January 25, 2013, I resumed my telephone calls with my mother, and noticed that my mother had ceased from asking beneficiary related questions").

Thus, whether there were questions about beneficiaries or not, that constituted confirmation in the applicant's eyes that the financial information had been accessed and disclosed. The evidence, however, shows that the only access took place after the beneficiaries' information had been deleted from the accounts. Similarly, the applicant sees further confirmation of disclosure in her mother's reaction when "confronted" in June 2013, as opposed to that being a strong reaction to some accusation proffered during a "confrontation". It seems that whatever happened, the applicant saw it as confirmation of her suspicions that her personal financial information had been disclosed to family members.

[27] I share the view expressed in the Privacy Commissioner's Report of October 21, 2015, that this does not constitute evidence on which such an allegation of disclosure can be confirmed. The evidence in this case is to the effect that the only access to the applicant's financial information occurred on February 24, 2013, well after January 25. The information about beneficiaries was available before January 25, 2013, but the information was not accessed by the RBC employee. Conversely, that information was not available when the conversations between the applicant and her mother resumed after that date, at which point the applicant contends that the lack of questions from her mother confirms that she now knew about the accounts. It is only a month later, on February 24, that the information was accessed. In effect, the applicant seems to have had suspicions whether or not the mother could have had access to the accounts. The Commissioner also notes that the allegation is based solely on a perceived change in the mother's behaviour. In the view of the Commissioner, there is not sufficient evidence to confirm disclosure given that "the complainant confirmed to RBC's CIS representative that her mother had never actually shared any specific information about the complainant's banking investments

with her, nor had her mother ever specifically questioned the complainant's choice of beneficiaries." The applicant is convinced that the RBC employee disclosed her financial information. Unfortunately for her, being convinced does not constitute evidence and, surely, it does not constitute clear, convincing and cogent evidence which satisfies the standard of proof of "balance of probabilities". During the hearing, the applicant contended that there was no evidence either that the RBC employee did not disclose the information. That submission does not account for the fact that it is the applicant who has the burden of proof which is discharged by evidence led by her that establishes disclosure on a balance of probabilities. Here, the RBC employee claimed on April 25, 2013, that she did not disclose the financial information which, at any rate, could not have been information about beneficiaries. That evidence was left unchallenged. Similarly, the strong reaction to the confrontation is in the view of the applicant further confirmation of knowledge. One is hard pressed to understand why. This cannot constitute clear, convincing and cogent evidence of disclosure.

[28] It follows that only the contravention to Principle 4.5 as to the use made of personal information is relevant to the proceedings before the Court. There was no unauthorized disclosure proven in this case. The relevant portion of Principle 4.5 reads as follows:

4.5 Principle 5 – Limiting Use, Disclosure, and Retention	**4.5 Cinquième principe – Limitation de l'utilisation, de la communication et de la conservation**
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall	Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne

be retained only as long as necessary for the fulfilment of those purposes.	l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.
[My emphasis]	[Je souligne]

Damages

[29] In effect, the proceedings launched pursuant to section 14 of PIPEDA are an attempt to be awarded damages resulting from the violation of the obligation to use the personal information for a purpose other than that for which it was collected and its disclosure. The use of personal information in this case is the access, which was not authorized, by an employee of RBC. There is no evidence that it happened more than once. In fact, the Commissioner's Report notes at para 36 that "once RBC realized that there had been an unauthorized access by the employee, it immediately took measures to begin monitoring any future access to the complainant's financial information by the employee". There is no evidence of disclosure. Thus, the issue is whether or not compensation ought to be paid by the respondent where the privacy violation is limited to one occurrence of use without further disclosure.

[30] Once a matter is before a court, it becomes adversarial. In the adversary system, the parties, and not the judge, have the primary responsibility for defining the issues in dispute and for carrying the dispute within the system (see *The Judge and the Adversary System*, by Neil Brooks, in The Canadian Judiciary, ed. by Allen M. Linden, , York University, (Toronto: Osgoode Hall Law School, 1976)). That requires that the truth-seeking process be largely in the hands of the parties (*R v Bradshaw*, 2017 SCC 35; [2017] 1 SCR 865, at para 19). That is true of parties represented by counsel or litigants in person. The role of the judge is limited. It may be

expected that an explanation of the process will be given, that there be inquiries of a litigant in person as to the understanding of the process and the procedure, that information about the law and the evidentiary rules be made available or even that questions be asked of witnesses in appropriate circumstances to clarify issues (Statement of Principles on Self-represented Litigants and Accused Persons, adopted by the Canadian Judicial Council in September 2003, and specifically endorsed by the Supreme Court of Canada in *Pintea v Johns*, 2017 SCC 23; [2017] 1 SCR 470). That is the kind of assistance that was offered in this case at the hearing. However, the judge cannot become a party to the proceedings. As Lord Sumption put it recently with respect to a litigant in person who had neglected to serve appropriately his claim, "[t]heir lack of representation will often justify making allowances in making case management decisions and in conducting hearings. But it will not usually justify applying to litigants in person a lower standard of compliance with rules or orders of the court" (*Barton v Wright Hassall LLP*, [2018] UKSC 12 at para 18). I would think that the some kind of rigour applies, perhaps even more so, to the burden of proof and the standard required in law to prove one's case. It is for an applicant to put her case forward.

[31] Accordingly, the adjudication in this case must be based on the case put forth by the applicant, and only with respect to "any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1 or 1.1, in subsection 5(3) or 8(6) or (7), in section 10 or in Division 1.1." (subsection 14(1) of PIPEDA). Here, the Privacy Commissioner addressed principles 4.5 and 4.7. It is inappropriate to seek to expand the scope of proceedings pursuant to section 14 to

include matters that were not complained of or not referred to in the Report and that is not referred to in various clauses of the Principles. The Court does not have jurisdiction if what is raised does not fall within the four corners of section 14 (*Nammo*, at para 25).

[32] The matter in respect of which the complaint was made and that is referred to in the Principles in Schedule 1 of PIPEDA is that which is found at Principle 4.5. The Commissioner also considered Principle 4.7. The proceedings are limited in that fashion. The applicant raises the damages that were caused to her by the disclosure of her financial information to family members. She writes that "(t)he irreconcilable damage with my family members has caused me a great deal of humiliation and embarrassment".

[33] The applicant also claims that RBC officials "dealt with this situation in an unethical, unprofessional, and uncaring manner". It is hard to see on the record before the Court any substantiation of these allegations. Indeed, it is less than clear in what fashion they relate to the Principles found in Schedule 1 of PIPEDA and for which an application to section 14 is apposite. It perhaps bears repeating that the obligations under PIPEDA are those found in the principles (subsection 5(1) of PIPEDA) and a complainant to the Privacy Commissioner can be made against an organization for a contravention of Division 1 of PIPEDA (section 11)). A different cause of action should be pursued in a different forum if it falls outside of the confines of section 14. Be that as it may, there was no evidence led which suggested, let alone proved, that RBC did not act appropriately in its review of the complaint. It was given some particulars of the person suspected by the applicant of improper access on March 18, 2013. On April 12, RBC reported that there had not been any such access in 2010, 2011 and 2012. The review continued to include

the first few months of 2013; on April 25, 2013, one improper access had been identified and the RBC employee was interviewed. The RBC employee confirmed the access but denied disclosure. Such is the evidence before the Court.

[34] Clearly, the applicant was interested in compensation for what she thought had been disclosure of some private information to her family very early in the process; however, there is uncontroverted evidence that the breach is limited to one unauthorized access without further disclosure. The applicant pursued compensation, which was not forthcoming, for the difficulties encountered with her family after the June 2013 confrontation. Already on September 3, 2013, she wrote to the office of the ombudsman complaining that the disclosure had caused her "insurmountable grief and irreconcilable damage with my family members". She was asking that the privacy breach be remedied ("RBC must make this wrong, right"). In fact, she seems to have taken strong issue with the response of a regional vice president of RBC dated September 24, 2013. In it, the Vice President acknowledges the access breach, apologizes, but does not offer any compensation. He also declined, for privacy reasons, to disclose how the RBC employee had been dealt with. In the view of this Court, that letter was courteous and appropriate.

[35] The applicant pursued the matter with a letter to the RBC office of the Ombudsman on October 9, 2013. The response came on January 13, 2014, in a two-page letter which reviewed in some details the compensation issue. We read that "(a)fter my review of your complaint, I have no basis for a recommendation for compensation". The applicant made again the same complaint to the Office of the RBC Chief Privacy Officer, this time on March 11, 2014. The response came

on March 19, 2014. It acknowledges that the matter has not been resolved to the applicant's satisfaction, yet "the Bank has completed a thorough review and considers the matter closed".

[36] The applicant has contended that she has received the "royal runaround". The Court has not found any evidence to that effect. As can be seen from the chronology of events, the respondent has shown diligence in its investigation as well as its response to the complaint made. Assuming that this response at different levels to the complaint may have constituted a violation of a principle, which is far from clear, there is nothing on this record to support an accusation that the situation was dealt with in an "unethical, unprofessional, and uncaring manner".

[37] As for the safety measures taken by the respondent (principle 4.7), they are dealt with in the Report of Findings of the Privacy Commissioner. These findings were not challenged by the applicant, even when prompted by the Court during the hearing of this case. Given the generality of the applicant's complaint and the lack of evidence adduced, there is no reason to doubt the conclusion at paragraph 37 that "the employee simply neglected to abide by the rules". The Privacy Commissioner declares that "we are satisfied with the corrective actions that RBC took vis-à-vis its employee at the centre of this complaint" (para 38), including the necessary disciplinary measures. That has not been challenged and I see no reason to depart from that finding.

[38] That leaves the issue of damages for this breach of Principle 4.5 for a single unauthorized access to financial information. In my view, the applicant has failed to prove that the

respondent's breach warrants damages in the order of $100,000.00 being awarded. These are my reasons for reaching that conclusion.

[39] The breach of privacy proven in this case is of the lesser kind. It is beyond discussion that privacy in relation to information deserves protection. Thirty years ago, the Supreme Court of Canada spoke in terms of dignity and integrity of the individual in *R v Dyment*, [1988] 2 SCR 417 [*Dyment*]:

> Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it (p. 13): "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained; see, for example, the *Privacy Act*, S.C. 1980-81-82-83, c. 111.
>
> (pp 429-430)
>
> [My emphasis]

Even in 1988, the concerns were not new. The Court in *Dyment* refers to a Task Force established jointly by the Department of Communications and the Department of Justice which produced a 184-page report under the title *Privacy and Computers* in 1972. The Federal Court of Appeal in *Information Commissioner of Canada v Canadian Transportation Accident Investigation and Safety Board*, 2006 FCA 157; [2007] 1 FCR 203, quotes with approval Justice

Brandeis who, 90 years ago, wrote in *Olmstead v United States*, 277 US 438 (1928) that privacy is the "right most valued by civilized men". This is high authority indeed.

[40] In the case at bar, an employee of the respondent had access to personal information without that access being for genuine business purposes; that is a violation of Principle 4.5, but it does not include any further disclosure. There is simply no evidence to that effect. Indeed, the applicant's suspicions that her mother had been made aware of the financial information appear to stem from conversations with her that took place before there was the impugned access. If the applicant's mother changed her behaviour, that was not, on the evidence in this case, because some information about her accounts came to her mother's attention: the person who had access to her information said she did not disclose further and that access came about on February 24, 2013, likely after the applicant had resumed her conversations with her mother where she noted a change in behaviour. Thus, the violation must be seen as being on the low end of the spectrum: as already noted, this is a case of an employee who "simply neglected to abide by the rules" (Report of Findings, para 37). In this case the contravention is very much limited in view of an absence of evidence of any dissemination. Although not much is known about the accessed information, we know that it is of a financial nature, not related to the health, welfare or personal choices. It does not even include information about beneficiaries. It is personal information of some sensitivity, but not deeply personal or intimate. It is private information that is "at the low end of sensitivity of personal information" (*Stevens v SNF Maritime Metal Inc.*, 2010 FC 1137 [*Stevens*], at para 20). As the Court put it in *Stevens*, it "must examine the real nature of the remedy claimed. Such claims as humiliation, loss of community support, diminution of standings and loss of income flowing therefrom (to name but a few) caused by breach of the Act fall within

the statutory cause of action created by the Act" (para 27). Because of the fact that there was no disclosure, these factors are not apposite. In fact, the claim is based on the damage caused to the family relationships because of disclosure to them. But there is no evidence that there was disclosure and the possible cause of the damaged family relationships may well be the confrontation of June 2013 when the applicant disclosed the access to her account by a family member.

[41] The leading case in this Court on the issue of damages pursuant to section 16 continues to be *Randall*:

> [55] Pursuant to section 16 of the PIPEDA, an award of damages is not be made lightly. Such an award should only be made in the most egregious situations. I do not find the instant case to be an egregious situation.
>
> [56] Damages are awarded where the breach has been one of a very serious and violating nature such as video-taping and phone-line tapping, for example, which are not comparable to the breach in the case at bar: *Malcolm v. Fleming* (B.C.S.C.), Nanaimo Registry No. S17603, [2000] B.C.J. No. 2400; *Srivastava c. Hindu Mission of Canada (Québec) Inc.* (Q.C.A.), [2001] R.J.Q. 1111, [2001] J.Q. no 1913.
>
> (See *Townsend v Sun Life Financial*, 2012 FC 550 [*Townsend*])

[42] Although the awarding of damages, as a discretionary matter, cannot be made lightly and should be made only in egregious situations, I am less than convinced that only in situations where there has been privacy breaches as serious as video-taping or phone-line tapping should there be serious consideration given to awarding damages. Rather, the examples given suggest that there must be a measure of seriousness to the breach, that every violation does not call for

damages to be granted, but the breach does not require to be as extreme as video-taping or wiretaps. The case law of this Court would tend to confirm that damages would still be payable when the behaviour falls short of such extremes.

[43] In this case, there was no malice on the part of the respondent. The respondent did not benefit from its employee's breach. It acted swiftly. There is no evidence of any disclosure. It readily acknowledged the breach and remedied it diligently. Furthermore, the applicant has been proven incapable of establishing the nature or the quantum of damages (*Soup v Blood Tribe Board of Health*, 2010 FC 955) other than the embarrassment and humiliation when she met her siblings and, more generally, the damage caused to her relationship with her family by an alleged disclosure as documented by the Behavioural Health Consultant. The problem with this is that, on the evidence presented in this case, there is no evidence of disclosure that could account for the damage to family relationships. Any disclosure is possibly, even likely, the result of the applicant confronting her mother in June 2013, shortly after she learned of the improper access to her financial information. The uncontradicted evidence is that there was no disclosure by the respondent or one of its agents: that is the conclusion reached by the Privacy Commissioner and the Court came to the same conclusion. There is simply no evidence to the contrary.

[44] The cases in which damages have been awarded seem to fall for the most part in the category of cases where private information was disclosed (*Landry v Royal Bank of Canada*, 2011 FC 687; *Nammo*, *supra*; *Girao v Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070 [*Girao*]; *Biron*, *supra*; *Chitrakar v Bell TV*, 2013 FC 1103; *Henry v Bell Mobility*, 2014 FC 555; *A.T. c Globe24h.com*, 2017 FC 114; 407 DLR (4th) 734 [*Globe24h.com*]). In *Cote v Day & Ross*

Inc., 2015 FC 1283, it was rather the refusal to disclose to the applicant personal information, possibly relating to a long-term disability issue Ms. Cote was pursuing with an outside insurer, which was in play.

[45] There is insufficient, indeed there is no evidence, that the hardship suffered, including humiliation and embarrassment, was caused by the respondent. It is the disclosure of the information which resulted in the family rift and the ensuing anxiety. We should nevertheless consider if damages ought to be awarded for the unauthorized access.

[46] There are two issues. First, there is a complete lack of support for damages once it is acknowledged that there has been no disclosure of the accessed information (*Kollar v Rogers Communications Inc.*, 2011 FC 452). The applicant has built her case from the start on the foundation that her financial information had been shared with her immediate family. She is convinced of that. Unfortunately, she has not proven disclosure, as she acknowledged during the hearing of the case. The evidence on damages offered by the applicant is that of the reports of a Behavioural Health Consultant. It is clear from reading the reports that it is the family relationships that were her concern, and caused the applicant to seek some assistance. Those relationships were damaged by the disclosure, not the unauthorized access. The applicant resorted instead to arguing that the respondent had not proven either that disclosure has <u>not</u> occurred. The burden, or onus, is, however, on the applicant. The burden on the applicant "is to the effect that damages should only be awarded in cases where they are substantially justified and would further the objectives of PIPEDA in ensuring that organizations are diligent in retaining as secure, personal information" (*Blum v Mortgage Architects Inc.*, 2015 FC 323, at

para 60). The evidence of damages to the family relationships caused by the respondent cannot hold without disclosure by the respondent and the evidence is lacking if the only violation is that one access to personal information on February 24, 2013 (*Bertucci v Royal Bank of Canada*, 2016 FC 332).

[47] Second, it has been suggested in some of this Court's case law that damages may be justified to compensate, deter or vindicate (*Nammo* (*supra*), *Townsend* (*supra*), *Girao*, (*supra*), *Globe24h.com* (*supra*)). As I have already indicated, there is no sufficient evidence to compensate damages caused by one unauthorized access. Given the circumstances of the case, one is hard pressed to find where deterrence is needed. It seems to me that the Report of Findings is dispositive (para 36 to 38 in particular) on that front.

[48] I would decline to award damages where no damages have been proven by the applicant as caused by a breach of PIPEDA. Indeed, the amount of damages sought is greatly out of proportion with the jurisprudence of this Court. Furthermore, the breach was not egregious in the absence of a disclosure outside the confines of the institution or in the absence of repetition. In my view, we should be concerned about not turning breaches of PIPEDA into an opportunity for vindication in the form of the imposition of an award of damages, even if merely nominal, every time a violation occurred. Vindication takes many forms. The statute speaks in terms of "may award damages", not that damages must be awarded if a violation is found. If damages are to be awarded in a case like this where there is no further disclosure, no benefit to the company which has taken appropriate steps to protect personal information and has imposed appropriate disciplinary measures proportional to the circumstances, that would suggest that the seriousness

of the breach is not a factor to consider as it has become inconsequential. I rather think that the discretion to award damages should be exercised where there is a measure of gravity to the breach which is often exemplified by disclosure of private information, but not always. Unauthorized access on a grander scale might satisfy the "seriousness" requirement. Here, the unauthorized access to financial information was immediately acknowledged by the respondent and confirmed as being a contravention to Principle 4.5 by the Privacy Commissioner (Report of Findings, para 32). That is vindication.

[49] Going back to section 3 of PIPEDA, Parliament recognized that privacy is deserving of protection where the circulation and exchange of information is facilitated by the technology. But the section also acknowledges "the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances". Organizations must be encouraged to take alleged violations of the PIPEDA principles seriously, investigate them, reckon violations when they occur and take appropriate measures. Here, the respondent had in place a robust system in order to prevent violations; once a violation was detected, measures were taken immediately, including the monitoring of the employee responsible for the unauthorized access. The applicant did not provide evidence of damages suffered by the sole violation that was identified and, in my estimation, this is not a case where discretion should be exercised in favour of granting damages.

[50] It goes without saying that exemplary or punitive damages are not apposite. There are no "advertent wrongful acts that are so malicious and outrageous that they are deserving of

punishment on their own" (*Honda Canada Inc. v Keays*, 2008 SCC 39; [2008] 2 SCR 362, at para 62). In *de Montigny v Brossard (Succession)*, 2010 SCC 51; [2010] 3 SCR 64, one reads:

> [47] While compensatory damages are awarded to compensate for the prejudice resulting from fault, exemplary damages serve a different purpose. An award of such damages aims at expressing special disapproval of a person's conduct and is tied to the judicial assessment of that conduct, not to the extent of the compensation required for reparation of actual prejudice, whether monetary or not. As Cory J. stated:
>
> > Punitive damages may be awarded in situations where the defendant's misconduct is so malicious, oppressive and high-handed that it offends the court's sense of decency. Punitive damages bear no relation to what the plaintiff should receive by way of compensation. Their aim is not to compensate the plaintiff, but rather to punish the defendant. It is the means by which the jury or judge expresses its outrage at the egregious conduct of the defendant.
> >
> > (*Hill v. Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130, at para. 196)

V. Conclusion

[51] In the adversary system of justice, it is the applicant's burden to satisfy the Court on a balance of probabilities that the respondent was responsible for the disclosure of the accessed information. There is a complete lack of evidence in that regard.

[52] Although it is recognized that there was a violation of Principle 4.5 in that there was one incident of one unauthorized access to some of Ms. Miglialo's financial information in the possession of the respondent, she equally had the burden of supporting her claim for damages

with evidence with a view to showing that damages were caused by the actions of the respondent. This is a case characterized by a lack of evidence. The applicant's whole case was based on the damage caused to her family relationships by the disclosure to her family of her private financial information which apparently resulted in some anxiety issues which required the assistance of a Behavioural Health Consultant. There was no evidence of such disclosure by the respondent, thus negating the causation between the breach and the alleged damages. The lack of evidence of "substantially justified" damages for the actual very limited breach of her privacy is fatal. This is not a case either for damages in order to deter negligence as the steps taken by the respondent to protect and deal with private information were found to be adequate by the Privacy Commissioner: nothing was presented to this Court to detract from that finding. Finally, the Court's discretion should not be exercised in favour of awarding even a nominal amount of damages without interfering with the principle that damages are not to be awarded lightly, and only in egregious situations. Vindication is to be found in the respondent's acknowledgement of the breach, which resulted in appropriate disciplinary measures, as well as the finding of the Privacy Commissioner that a violation of Principle 4.5 occurred.

[53] The respondent is not seeking costs and, thus, none are awarded.

JUDGMENT in T-1424-16

THIS COURT'S JUDGMENT is that:

1. The application is dismissed;

2. There will not be an award of costs.

"Yvan Roy"

Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-1424-16
STYLE OF CAUSE:	ANGELA MIGLIALO v ROYAL BANK OF CANADA
PLACE OF HEARING:	CALGARY, ALBERTA
DATE OF HEARING:	MAY 8, 2018
JUDGMENT AND REASONS:	ROY J.
DATED:	MAY 22, 2018

APPEARANCES:

Angela Miglialo	FOR THE APPLICANT (ON HER OWN BEHALF)
Jordan R.M. Deering	FOR THE RESPONDENT

SOLICITORS OF RECORD:

Norton Rose Fulbright Canada LLP Barristers and Solicitors Calgary, Alberta	FOR THE RESPONDENT