Federal Court  Cour fédérale

Date: 20230203

Docket: T-1335-22

Citation: 2023 FC 166

Ottawa, Ontario, February 3, 2023

PRESENT: The Honourable Mr. Justice Roy

BETWEEN:

TAMARA JAMES

Applicant

and

AMAZON.COM.CA, INC.

Respondent

JUDGMENT AND REASONS

I. Overview

[1] The *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, better known as PIPEDA, is legislation created for the protection of the personal information. As section 3 of PIPEDA spells out, it aims to balance the protection of personal information while allowing organizations to collect, use or disclose personal information. Section 3 reads as follows:

Purpose	**Objet**
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 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.	**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 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.

[2] The Applicant, a litigant in person, invokes PIPEDA to gain access to the personal information held by the Respondent, Amazon.com.ca, Inc. (hereinafter "Amazon"). She says that it is her personal information. Amazon claims that it is prevented by PIPEDA from disclosing to the Applicant the personal information it holds until and unless it has been able to authenticate that the person seeking access is the person who is entitled to it. As can be seen, the sad irony is that both parties rely on PIPEDA for purposes diametrically opposed: one claims that PIPEDA creates an obligation to disclose to her while the other party claims it cannot disclose without being in violation of the same PIPEDA.

[3] The Applicant, Ms. Tamara James, brings her dispute with Amazon before this Court pursuant to section 14 of PIPEDA:

Hearing by Court

Application

14 (1) A complainant may, after receiving the Commissioner's report or being notified under subsection 12.2(3) that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of 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.

Time for application

(2) A complainant shall make an application within one year after the report or notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.

For greater certainty

(3) For greater certainty, subsections (1) and (2) apply in the same manner to complaints referred to in subsection 11(2) as to complaints referred to in subsection 11(1).

Audience de la Cour

Demande

14 (1) Après avoir reçu le rapport du commissaire ou l'avis l'informant de la fin de l'examen de la plainte au titre du paragraphe 12.2(3), le plaignant peut demander que la Cour entende toute question qui a fait l'objet de la plainte — ou qui est mentionnée dans le rapport — et qui est visée aux articles 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 ou 4.8 de l'annexe 1, aux articles 4.3, 4.5 ou 4.9 de cette annexe tels qu'ils sont modifiés ou clarifiés par les sections 1 ou 1.1, aux paragraphes 5(3) ou 8(6) ou (7), à l'article 10 ou à la section 1.1.

Délai de la demande

(2) La demande est faite dans l'année suivant la transmission du rapport ou de l'avis ou dans le délai supérieur que la Cour autorise avant ou après l'expiration de l'année.

Précision

(3) Il est entendu que les paragraphes (1) et (2) s'appliquent de la même façon aux plaintes visées au paragraphe 11(2) qu'à celles visées au paragraphe 11(1).

[4] In *Miglialo v Royal Bank of Canada*, 2018 FC 525 [*Miglialo*], I commented in the following fashion about the Court's role in determining an application under section 14 of PIPEDA and the burden of proof:

> [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.

It follows that the burden is on the Applicant to show a violation of PIPEDA on a balance of probabilities, using evidence that is clear, convincing and cogent. Cases usually are concerned with disclosure of information that is unauthorized. Such is not the case here.

[5] Moreover, the ability of the Court to entertain matters pursuant to proceedings under section 14 is limited by the section itself (*Miglialo*, at para 31). It must be concerning a matter in

respect of which the complaint before the Privacy Commissioner was made, or it could be in respect of a reference made in the Commissioner's Report. It would be inappropriate for an applicant to seek to go beyond the parameters of section 14.

II. The Facts

[6] The Applicant, Ms. Tamara James, claims that she became a customer of the Respondent after creating an account online with Amazon (the "Account").

[7] The Respondent is an online retailer in Canada. The Respondent carries on business as a subsidiary of its American affiliate Amazon.com, Inc. Amazon.com, Inc. is incorporated under the laws of Delaware, and has its headquarters located in Seattle, Washington (Applicant's record, p 162).

[8] On August 15, 2020, the Applicant claims that she used the Account to purchase an Amazon Prime membership to renew on a monthly basis (Applicant's record, p 19). It appears that the Applicant forgot the password associated with the Account.

[9] On August 31, 2020, the Applicant contacted Amazon via telephone after unsuccessful attempts to log in to the Account. She was advised that her identity could not be authenticated because the name, email, and mailing address she provided did not correspond with the information contained on the Amazon's server (Applicant's record, p 14). That day, she emailed Amazon's customer service portal to request assistance with accessing her account. She also

sought to change her password and cancel her Prime membership subscription (Applicant's record, p 19).

[10] On September 1, 2020, the Applicant tried to recover her password twice by following Amazon's two-factor authentication service. This involved requesting a One-Time Password (OTP) through the email address associated with the Account (Applicant's record, pp 21-22). The Applicant claims that when she entered her OTP to authenticate herself, the Amazon website directed her to contact its customer service representatives by telephone (Applicant's record, p 14).

[11] On September 2, 2020, the Applicant sent a letter via email to the customer service portal and by regular post to Amazon's corporate headquarters in Seattle, Washington (Applicant's record, pp 24-25). In the letter, the Applicant requested access to: (1) all of the information associated with the Account, (2) receipts from the transactions on the Account between August 10, 2020 and August 26, 2020, and (3) audio recordings of all her prior dealings with Amazon's customer service representatives (Applicant's record, p 25). An Amazon representative emailed her back that day, inviting her to access the requested invoices by logging into the Account. The representative also informed her that Amazon does not provide recordings of phone calls to its customers (Applicant's record, p 26).

[12] By email dated October 22, 2020, the Applicant advised Amazon that it had a 30-day time limit to respond to her access for information request (Applicant's record, p 28). She received a responding email that day, in which an Amazon representative asked for more

information about the Applicant's past purchases (Applicant's record, p 29). Nothing in the record suggests that the Applicant responded to this request.

[13] On November 2, 2020, the Applicant filed a formal privacy complaint with the Office of the Privacy Commissioner of Canada (the "Commissioner"). She summarized her complaint in the following terms:

> Amazon.com Inc is refusing to provide me with access to my personal information and refuses to provide receipts of online purchases requested in writing on September 2 2020.
>
> (Applicant's record, p 33.)

[14] In response to the question "What would resolve your complaint for you?", the Applicant wrote: "Access to information requested, including copies of all receipts and copies of all my personal information held by Amazon.com Inc." (Applicant's record, p 33).

[15] The Applicant attached four documents to her formal complaint. Two of the documents are copies of the email and letter dated September 2, 2020, in which Ms. James initiated her request for access to the information associated with the Account. A third document is Amazon's customer service representative's email response to her request which she received on September 2, 2020 at 10:29 a.m. The final document is the Applicant's follow up email dated October 10, 2020, in which the Applicant advised Amazon that it had 30 days to respond to her request.

[16] On November 10, 2020, an agent for the Privacy Commissioner responded to the Applicant's complaint letter, instructing her to send her request to the Amazon Privacy Officer

before pursuing her complaint with the Commissioner (Applicant's record, p 35). The Commissioner provided the Applicant with the mailing address for Amazon's Chief Privacy Officer and noted that if the issue was not resolved to her satisfaction, she could still pursue the complaint with the Commissioner provided that she deliver copies of correspondence between her and Amazon's Privacy Officer (Applicant's record, p 35).

[17] On November 13, 2020, the Applicant submitted her request to the Amazon Privacy Officer, using the address provided by the Privacy Commissioner (Applicant's record, p 37). The record does not show whether Amazon responded.

A. *The Disputed CIBC Credit Card Transaction*

[18] In an affidavit made in support of her application (Applicant's record, p 15), Ms. James states that on November 22, 2020, she disputed "all of the credit card transactions" related to her Amazon subscriptions from September to November 2020 (Applicant's record, p 15, para 14). The record does not show how she raised her concerns with CIBC or what were the contested purchases. Ms. James attaches a seven-page exhibit ("Exhibit H") to this section of her affidavit, which appears to include pages from several documents relating to one purchase the Applicant challenged with CIBC (Applicant's record, pp 39-45).

[19] The first two pages of Exhibit H consist in a letter from CIBC addressed to "Tashesha James" dated December 11, 2020. CIBC wrote that it was following up on the Applicant's request to challenge a $17.32 purchase for a product that was billed to her CIBC credit card on November 22, 2020. CIBC advised the Applicant that it would temporarily reimburse credit back

onto her account and enclosed a copy of the transaction receipt that Amazon had provided to CIBC upon its request. CIBC provided two possible courses of action for Ms. James to pursue. Either she could dispute the transaction by completing an attached "Dispute Letter" by December 26, 2022, or, should she decide not to reply, CIBC would consider the matter resolved and remit the purchase back onto her credit card (Applicant's record, p 39). The record is silent as to what developments there were.

[20] The next three pages of Exhibit H appear to be the copy of the Applicant's bank statement and Amazon's Merchandise Order Receipt ("Receipt") relating to the transaction at issue. One detail emerges from this document. The Receipt states that the customer who purchased the product initiated the subscription order for the product on Saturday, November 7, 2020:

> This order was placed automatically through an active Subscribe & Save subscription initiated by the customer on [Saturday, November 7, 2020]. (Applicant's record, p 42.)
>
> Order Placed Date and Time: Sat, Nov 7, 2020 02:41 PM PTS. (Applicant's record, p 43.)
>
> [My emphasis.]

[21] Although the subscription was ostensibly initiated on November 7, 2020, the transaction date for the order appeared to be on November 22, 2020, the same day that the order was shipped to the Applicant's residence. The product was delivered to the Applicant's residence on November 23, 2020.

[22] The evidence offered by the Applicant on that transaction is sparse. At the hearing and in her factum (para 32), the Applicant claimed that she had initiated the purchase on a monthly basis prior to her being locked out of the Account (i.e. prior to August 31, 2020). That may be so. However, nowhere in the materials does the Applicant provide evidence to substantiate the assertion. Nor is there evidence to the effect that Amazon charged her on an ongoing basis (before or after November 22, 2020). The Applicant did not provide any explanation as to how the subscription was "initiated" on November 7, 2020 as the document offered in evidence asserted, a time where she claims that she was blocked from accessing the Account. In other words, the evidence is incomplete and unclear with respect to that one transaction. Moreover, it remains unanswered whether the Applicant escalated the disputed transaction in accordance with the instructions set out by CIBC's letter and what role, if any, the Respondent played in the resolution of the issue.

[23] The Receipt also provides that Amazon successfully delivered the merchandise to the cardholder. The "Notes" section of the Receipt states (Applicant's record, p 42):

> The merchandise was delivered to the verified address of the cardholder. The cardholder's billing information matches the shipment information provided at the time the order was placed. Please review this information with your customer as this order appears to have been placed by someone with authorized access to the account.
>
> The customer has successfully used this shipping address for 8 number of orders that were previously processed and are not disputed. This suggests the address is authorized by the customer.

In effect, it is unclear what that evidence shows other than Amazon was instrumental in delivering a product to someone living at the address given. CIBC appears to have

communicated with “Tashesha James” who holds a CIBC credit card. Who ordered the product billed to the credit card is unknown, although a receipt for shipment indicates that the billing address is that of “Tashesha James” and the shipping address is that of “Tamara James”: both addresses are the same. At the hearing, the Applicant indicated she uses both names. Nevertheless, the documentation offered in evidence is careful to refer to the cardholder being the customer who provided the billing address. The customer is Tashesha James. Without more information about the dispute, such as who placed the order and when, who is the cardholder and what were the instructions given, the information provided by the Applicant concerning Amazon’s involvement is of limited use. In fact, the information does not contribute to enlightening a trier of fact.

B. *The Privacy Complaint at Issue*

[24] The complaint to the Privacy Commissioner of November 2, 2020 was made the subject of a reply by the Privacy Commissioner on November 10, 2020 (Applicant’s record, p 35). The suggestion was made therein for the Applicant to contact the Amazon Privacy Officer. That appears to be in line with section 12 of PIPEDA. Indeed, the Applicant followed up with a letter to the Chief Privacy Officer on November 13, 2020.

[25] Having directed the Applicant to contact Amazon Privacy Officer in November 2020, a privacy investigator for the Office of the Privacy Commissioner contacted the Applicant on June 9, 2021 to find out whether she still intended to pursue her complaint against Amazon. The Applicant confirmed that she did. It looks like that, other than the letter to the Chief Privacy

Officer of Amazon of November 13, 2020, the Office of the Privacy Commissioner was not aware of developments, if any, between November 2020 and June 2021.

[26] On June 23, 2021, the Applicant received an email and phone call from "Eugenia S.", an Amazon Executive Customer Service representative who was assigned to her file (Applicant's record, p 52). The Applicant responded to this email two months later apparently, on August 31, 2021 (Applicant's record, p 52). She attached the letter dated November 13, 2020 requesting access to the personal information associated with the Account.

[27] From September 15 to September 22, 2021, the Applicant corresponded with two members of the Amazon's Executive Customer Relations team. The Applicant informed them that the issue related to her "invoices" was resolved (Applicant's record, p 54). The details as to the resolution are lacking, including possible Amazon's involvement, if any. However, she still sought access to the personal information held by Amazon on the Account, and again requested copies of audio recordings between her and Amazon customer service representatives (Applicant's record, p 54).

[28] There were a number of interactions between Amazon and the Applicant, including with a lawyer from Amazon dealing with privacy compliance. Thus, the Respondent's record shows two emails on September 22, 2021 where Amazon counsel reaches out to Ms. James in a further attempt to resolve the issue. The first email bears the date of September 22, 2021, at 14:22:

> I understand that our Executive Customer Care team has been in touch with you regarding your access request. I wanted to personally reach out to let you know that I am working closely with the Executive Customer Care team, and to see how else I can

> be of assistance. Is my understanding correct that you would still like to submit a request for your personal information, but have been unable to verify your identity so as to gain access to your account?

The second email of the same day came at 17:02:

> My team is responsible for privacy compliance. I am an attorney that supports Amazon.ca and Amazon.com. Nicole with the OPC previously provided us with your letter, and we have been trying to follow up with you on this request. We are more than happy to assist you, but we must verify your identity for privacy and security reasons before we grant you access to personal information. Would you like to arrange a call with me and a customer service representative to begin that process? Please let me know when you are available next week, and I will gladly arrange a time.
>
> (Respondent's record, p 15.)

[29] As can be seen from the second email message of September 22, 2021, the Applicant received an email from a Privacy Officer at Amazon, part of their legal team, who proposed arranging a call between herself, the Applicant, and a customer service representative. The Privacy Officer noted:

> We are more than happy to assist you, but we must verify your identity for privacy and security reasons before we grant you access to personal information.
>
> (Applicant's record, p 62.)

[30] A phone call was scheduled for, and took place on, September 29, 2021. On the call, the Applicant was informed that since she could not remember her password, she could gain access by resetting her password, a process that involved agreeing to Amazon's updated Terms of Service. In an email that the Applicant sent to the Privacy Commissioner in late afternoon on

October 12, 2021, after she was advised earlier that the complaint would not be pursued by the Privacy Commissioner, the Applicant describes her version of events on the call as follows:

> On September 29, 2021 at exactly 1:30pm, I spoke with a representative for Amazon concerning this matter. That conversation was recorded and should be available upon request. The additional information that the representative asked for a password, which I could not provide as I do not remember the password to the account. For me to gain access to the account in question at this time, I will be required to agree to Amazon's updated Terms of Service. My refusal to agree to Amazon's continued collection of my personal data is not a valid reason to deny access to already existing data.
>
> (Applicant's record, p 66.)
>
> [Emphasis added.]

[31] As we shall see later, it is unknown why the Terms of Service might be an issue. The Respondent's Privacy Officer had explained in a long email message to the Applicant (Applicant's record, p 64) of that same October 12, that Amazon could not grant the requested information because the Applicant was unable to authenticate the correct name of the account holder, and the mailing/billing address associated with the Account. The Amazon Privacy Officer also noted that during their September 29, 2021 phone call, the Applicant refused to provide additional information, indicated she did not want a customer service representative to call her back, and did not want to proceed with a self-service option. The Privacy Officer offered to assist the Applicant. She concluded her email of October 12, 2021 by providing the Applicant a clickable hyperlink to reset her password, should she wish to do so. She was advised that once she has been able to obtain her personal information, she could close her account and delete her information. The three paragraphs from the email are reproduced:

> I am writing in response to your letters dated 11/13/2020 and 9/22/2021, in which you request access to personal information

> associated with the email address REDACTED. First, I want to apologize for any confusion, frustration or difficulty that you have experienced. I understand that you had a very negative experience and I want to assure you that we have taken your feedback into account and are deep-diving ways to improve the customer experience associated with information requests.
>
> Unfortunately, we cannot grant you access to the information you have requested because we cannot verify your identity. On calls with your customer service representatives, you were unable to verify the name of the account holder and the mailing or billing address associated with the account. When we spoke on 9/29, you indicated that you did not wish to provide additional information, did not want a customer service representative to call you back, and did not want to proceed with our self-service options. If you change your mind, I am happy to assist you.
>
> For reference, you can change the password to your account using your email address by following the instructions here. Once your password is changed and you can login to your account, you can go to our Request Your Personal Information help page and follow the instructions to have a copy of your personal information emailed to you. You can also request the closure of your account and the deletion of your personal information.
>
> [Emphasis in the original.]

[32] The Privacy Commissioner investigator had been copied on the email from Amazon to the Applicant on October 12, 2021. That is when she informed the Applicant that the Commissioner would not investigate further her complaint. Given that the Applicant was unable to provide the information requested by Amazon, the Privacy Commissioner investigator believed that it was "fair and reasonable that an organization [authenticate] an individual before giving information on an account" (Applicant's Record, p 66). The investigator's email of October 12 states that "Unfortunately since you were unable to provide the information, we will not pursue with this complaint". A follow up email, further to the Applicant's late afternoon email response, referred to in paragraph 30 of these reasons for judgment, was sent on

October 13, 2021 by the Privacy Commissioner investigator, suggesting that the Applicant collaborate with Amazon to reset her password and obtain access to her personal information (Applicant's record, p 67). The October 13 email reads:

> Following the email you sent me yesterday, I had a telephone conversation today with Amazon's Privacy Officer. She said that she personally informed you by telephone on her personal cel [sic] phone since she works from home (not recorded) why they could not authenticate you. She confirmed that the information you have provided to her colleague does not match what they have on file so they could not authenticate you. Since that information did not match, they required your password which you said you did not remember it. For that reasons they suggested that you reset your password as indicated in her email to you dated September 28, 2021.
>
> Ms. James, we suggest that you collaborated with Amazon and reset your password and then you will be able to access your personal information. Our Office does agree that organizations needs [sic] to authenticate individuals to protect them if a third party tries to access their personal information.

[33] By an email dated October 16, 2021, the Applicant informed the Privacy Commissioner investigator that she would seek a reconsideration of the Commissioner's decision. I reproduce in its entirety the email sent by the Applicant to the investigator. It appears to encapsulate the Applicant's position:

> Since September 2020, I have made numerous attempts to authenticate my identity by providing personally-identifiable information associated with the account in question, including full name, current and previous mailing addresses, telephone number and email.
>
> On 11 December 2020, Amazon was able to resolve a dispute related to a credit card transaction by proving to my credit card provider that an item had been successfully delivered to Tamara James at the very address which it now falsely claims cannot be authenticated. If the information on the account was modified in any way, it was done so without my knowledge and is likely the result of an error on the part of Amazon.com.

> After refusing for several months to respond to my request for access, Amazon now asks that I reset the password on the account and accept its updated Terms of Service in order to authenticate my identity and to access the information requested. However, as I have no interest in using the services of Amazon.com, I cannot accept the updated Terms or consent to the continued collection of my personal information by Amazon.com.
>
> So, according to Amazon, and the OPC agrees, I cannot access my personal information unless I agree to use Amazon's automated online service; to access that service, I must authenticate my identity by using only a password; and to obtain that password, I must first authenticate my identity, which I am not able to do as Amazon continues to claim that none of the information that I have provided can be authenticated.
>
> As the OPC fails to comprehend the inherent flaws in Amazon's policy regarding privacy and access to information and has therefore declined to investigate the complaint without valid reason in accordance with section 12(1) of *PIPEDA*, I will be seeking reconsideration of the decision. Thank you.
>
> (Applicant's record, p 68.)

The Applicant did not address how the Terms of Service are in issue as the point was made by Amazon's Privacy Officer in the last email to Ms. James, on October 12, that she could request the closure of her account and delete the personal information. She does elaborate either on how the dispute over the credit card charges was resolved.

[34] On November 9, 2021, the Applicant submitted a "Request for Reconsideration" of the Commissioner's decision to decline to investigate her complaint (Applicant's record, pp 70 to 73). There is no indication that a reconsideration was even conducted.

III. What does the Complaint say?

[35] As already seen, the contents of a complaint are an essential parameter concerning the jurisdiction of this Court to hear a matter pursuant to section 14 of PIPEDA. The complaint to the Privacy Commissioner (section 12 of PIPEDA) was framed in the following fashion (Applicant's record, pp 32-33). The form filled out by Ms. James, which constitutes the complaint, specifically refers to being denied access to her personal information by Amazon.com, Inc., headquartered in Seattle, Washington. Ms. James indicates that she made requests on three dates: August 31, 2020, September 2, 2020 and October 22, 2020. It appears that the most relevant date is September 2 as the Applicant summarizes her complaint to the Privacy Commissioner: "Amazon.com, Inc. is refusing to provide me with access to my personal information and refuses to provide receipts of online purchases requested in writing on September 2, 2020". That appears to be the core of her complaint, as the record shows.

[36] We learn of some of the details in the section of the complaint dedicated to attempts made to resolve the issue. Thus, the Applicant claims that she attempted to contact Amazon starting on August 28, 2020 to gain access to information in possession of Amazon; she was told that her mailing address could not be verified. On September 2, 2020, the Applicant wrote to Amazon Corporate Headquarters, in Seattle, asking for copies of receipts for purchases between August 10 and August 26, 2020, as well as audio recordings of telephone communications between August 30 and September 1, 2020 involving her and Amazon's customer service team. The Applicant referred to a particular email address. She also referred directly to Principle 9 of

PIPEDA, as well as to the obligation for organizations, such as Amazon, to provide access to personal information within 30 days.

[37] The complainant acknowledges she received a response from Amazon the same day the request for personal information was made (September 2, 2020). It seems that the communication was to the effect that the mailing address given by the Applicant to verify before giving access to the account was not satisfactory in order to verify properly. On October 22, 2020, the Applicant again provided addresses (her current address and a previous one). Amazon replied to her email. The Applicant contends in her complaint to the Privacy Commissioner that "(i)t is a well known fact that Amazon.com, Inc. collects and stores extensive data on all its customers. It is not at all possible that Amazon.com, Inc. is unable to locate my personal information using either the email address or the mailing address that I provided". I note that the reply email of Amazon asked for it be provided with the "order information like (Order ID, product name, when the order was placed and amount that has been paid for the order), using this information we could easily able [sic] to locate the order" (Applicant's record, p 29). Ms. James says in her complaint that this kind of information was not available to her because "I was not provided with neither receipts nor email confirmation of my orders".

IV. The Case for the Applicant

[38] Ms. James seeks, among other things, a declaration the purpose of which is to compel the Respondent to comply with clauses 4.6.1, 4.6.3, 4.9.4 and 4.9.5. The Applicant alleges violation of two principles: denial of access to her personal information and the right to accurate information. She also seeks the payment of $218.12 which she calls compensatory damages, but

are in reality her disbursements. Exemplary damages situated at .001% of the net income of the Respondent for the quarter ending on June 30, 2022, “for ethical and deliberately deceptive privacy practices” were sought. Neither party was able to communicate to the Court what that amount may be. Be that as it may, the Applicant relented from that amount at the hearing of the case.

[39] Although the Notice of Application does not refer specifically to section 8(3) of PIPEDA, which sets a limit of 30 days to respond to a request, with the possibility of an extension (section 8(4) of PIPEDA), it refers generally to contravention of Division 1 of PIPEDA, where section 8 is located. Furthermore, some of the material appended to the formal complaint refers to timeliness.

[40] The Applicant’s contention is that she did not receive her personal information within a reasonable time (clause 4.9.4) or no more than thirty days after receipt of the request (section 8(3)) if there is no extension of time limit in accordance with section 8(4).

[41] The Applicant notes that she made three written requests over time (September 2, 2020; November 13, 2020; September 22, 2021) for access to private information. The three letters are identical except for the signature block of the third letter that uses the name “Tashesha Tamara James”. There is no explanation for that change. As already stated, at the hearing, Ms. James confirmed using both names. Actually, an examination of the record reveals that the Applicant seems also to have used two different email addresses to communicate with the Respondent. It appears that she changed address at some point.

[42] Ms. James was in fact in contact with customer service representatives very soon after her initial request in September 2020. However, the record shows that, throughout, the Respondent was not able to verify that this Applicant was entitled to access the personal information it held with respect to a particular account. As already alluded to, the record does not show why that was. There was no information that was provided by either party as to what was the content of the various interactions between the Applicant and the Respondent's representatives. That continues to be a mystery. Nevertheless, in effect, the Applicant received a response within the initial 30 days: she was not left with no response. However, she did not receive the information she was seeking.

[43] The Applicant's argument is that "none of the customer service representatives who communicated with the Applicant were designated to act on behalf of a privacy officer, nor were they even aware of the organization's policies and procedures for handling written requests" (memorandum of fact and law, para 23). That is why, says the Applicant, the communications are not a legitimate response to the complaint. No authority for that proposition was offered.

[44] Next, it is argued that the Respondent did not comply with Principle 6 which is concerned with the accuracy of personal information. Ms. James is right that the Principles set out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, which are found in schedule 1 to PIPEDA, must be complied with (section 5 of PIPEDA). A violation of Principle 6 is covered by section 14 of PIPEDA. As I pointed out during the hearing of this case, the emphasis is of course on the protection of personal information in PIPEDA, but

there is a requirement that the personal information be kept accurate. The Applicant sought to rely on Principle 6. I reproduce Principle 6 in its entirety:

4.6 Principle 6 — Accuracy	**4.6 Sixième principe — Exactitude**
Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.	Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés.
4.6.1	**4.6.1**
The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.	Le degré d'exactitude et de mise à jour ainsi que le caractère complet des renseignements personnels dépendront de l'usage auquel ils sont destinés, compte tenu des intérêts de la personne. Les renseignements doivent être suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements inappropriés soient utilisés pour prendre une décision à son sujet.
4.6.2	**4.6.2**
An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.	Une organisation ne doit pas systématiquement mettre à jour les renseignements personnels à moins que cela ne soit nécessaire pour atteindre les fins auxquelles ils ont été recueillis.
4.6.3	**4.6.3**
Personal information that is used on an ongoing basis, including information that is disclosed to third parties,	Les renseignements personnels qui servent en permanence, y compris les renseignements qui sont

should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.	communiqués à des tiers, devraient normalement être exacts et à jour à moins que des limites se rapportant à l'exactitude de ces renseignements ne soient clairement établies.

[45] The argument seems to be that since the Applicant cannot authenticate the connection between herself and the account at Amazon, it must be that the information held by Amazon is inaccurate. That, claims the Applicant, constitutes a violation of Principle 6.

[46] On this record, and purely factually, the Court has not been able to find any support in the evidence for what may be referred to as speculation if not supported by evidence. Ms. James in effect speculates that, if she was not able to gain access to what she says is her Amazon account, it must be because the Respondent did not have accurate information. It is certainly possible that the information held by Amazon is not accurate. However, the evidence in support is not part of this record. The Applicant suggests in her memorandum of fact and law that she requested assistance to determine what personal information had been modified, when and by whom the information had been modified, and to rectify the errors (para 31). I have reviewed the paragraphs from the Applicant's affidavit which she cites in support of her statement in the factum, together with the exhibits associated with those paragraphs (8 to 13) of the affidavit. They do not bring any evidence that could support the contention.

[47] Furthermore, the Applicant seeks to find support in the fact that Amazon shipped an item to the address claimed not to match the information associated with the account. That, argues the

Applicant, constitutes proof that she is the person who should be given access to the personal information.

[48] As I have already noted, it is very much unclear what the episode referred to establishes. It appears a transaction using a bank's credit card held by "Tashesha James" was challenged. The transaction was apparently with Amazon. The documentary evidence shows that the product was shipped to an "address provided by the customer when placing the order". The customer is the person with the Amazon account. However, the documentation carefully states that the customer and the shipping address are two different things. One reads the following:

> The merchandise has been shipped to the cardholder's verified billing address. Please have your customer carefully review the documentation provided as this order appears to have been placed by someone with authorized access to the account.
>
> NOTE:
>
> → The merchandise was delivered to the verified address of the cardholder. The cardholder's billing information matches the ship to information provided at the time the order was placed. Please review this information with your customer as this order appears to have been placed by someone with authorized access to the account.
>
> → The customer has successfully used this shipping address for 8 number of orders that were previously processed and were not disputed. This suggests the address is authorized by the customer.
>
> (Applicant's record, pp 42-43.)

[49] These mentions would suggest that it cannot be taken for granted that the shipping address (or billing address) corresponds to the customer who has the authorized access to the account. The point is made on four occasions. I add that there is no explanation why this order was challenged and what the details of the resolution of the dispute are.

[50] In the end, this partial information does not elucidate the connection between the Applicant and the Amazon account. Indeed not much is revealed about the transaction and the challenge. The lack of evidence hampers the ability of the Applicant to rely on the so-called CIBC credit card transaction.

[51] Ms. James puts forth the following proposition at paragraph 36 of her memorandum of fact and law: “If inaccurate identity data was, in fact, preventing the Applicant from accessing the account, Amazon’s refusal to address the inaccuracy issue is a clear and deliberate breach of the Accuracy Principle”. The Applicant is rightly careful in putting the proposition forward: she says “if inaccurate identity data” caused her to be incapable to have access, the Accuracy Principle may be engaged. But that constitutes the very thing that must be proven: was the personal information inaccurate? That is likely because the cause of the disconnect between the Applicant and the account has not been established to be the inaccuracy of the identity data. In the end, we do not know what caused the disconnect, if any.

[52] The next argument raised by the Applicant is a violation of Principle 9. In fact, that is the violation referred to directly in the complaint and addressed in the Report of Findings. In her notice of application, the Applicant refers more specifically to clauses 4.9.4 and 4.9.5. I reproduce the general principle requiring access and clauses 4.9.4 and 4.9.5. The whole text of Principle 9 is in an annex to these reasons:

4.9 Principle 9 — Individual Access	**4.9 Neuvième principe — Accès aux renseignements personnels**
Upon request, an individual shall be informed of the	Une organisation doit informer toute personne qui

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.	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 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.	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 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.
…	[…]

4.9.4	**4.9.4**
An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.	Une organisation qui reçoit une demande de communication de renseignements doit répondre dans un délai raisonnable et ne peut exiger, pour ce faire, que des droits minimes. Les renseignements demandés doivent être fournis sous une forme généralement compréhensible. Par exemple, l'organisation qui se sert d'abréviations ou de codes pour l'enregistrement des renseignements doit fournir les explications nécessaires.
4.9.5	**4.9.5**
When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.	Lorsqu'une personne démontre que des renseignements personnels sont inexacts ou incomplets, l'organisation doit apporter les modifications nécessaires à ces renseignements. Selon la nature des renseignements qui font l'objet de la contestation, l'organisation doit corriger, supprimer ou ajouter des renseignements. S'il y a lieu, l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question.

[My emphasis.]

[53] It looks like the argument is that Amazon's refusal to grant the Applicant access to personal information constitutes a violation of the principle. Because access is denied, the Applicant claims she is prevented from challenging the accuracy of the information held by the

Respondent. The Applicant did not address the "Note" in the chapeau of Principle 9. It provides for exceptions to the Access Principle, *inter alia*, where the disclosure cannot be effected because it is about "information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege". Clearly, the Applicant did not receive what she asked for. That she argues constitutes a violation of her right to access the personal information she claims is hers. However, she did not address whether the exceptions apply to her situation.

[54] Under the heading "Amazon failed to address the issues raised in the complaint", the Applicant seeks to argue about an issue that does not fall within the four corners of section 14: she claims that Amazon uses an "automated data request system" to make important decisions which should be left to human decision makers. The failure to do so somehow constitutes a failure to meet the obligations.

[55] She seeks a declaration that the Respondent's "artificial intelligence (AI) – based and automated decision-making (ADM) data request process does not comply with PIPEDA". This is in the nature of an attempt to explain why the Respondent was enable to authenticate.

[56] The issues under that general heading should be disposed of quickly. This issue cannot be made the subject of a recourse under section 14 of PIPEDA. Not only are we outside the scope of section 14, but the matter was not raised in the complaint, was not addressed by the Privacy Commissioner and there is no basis in the record to entertain an argument around artificial intelligence as an explanation for why access was denied.

[57] Furthermore, under the same general heading, Ms. James takes aim at what she refers to as “Amazon’s data request policy” which she claims does not comply with PIPEDA. The so-called “Policy” is presented this way at paragraph 52 of the Applicant’s memorandum of fact and law: “… Amazon’s data request policy requires that all requests for data be made digitally through its automated process”. The Applicant does not indicate what is the source of the contention that there exists such policy. On the contrary, various representatives engaged with the Applicant over time. It is rather that, for the safety of personal information, the law specifically provides that “the methods of protection should include technological measures, for example, the use of passwords and encryption” (clause 4.7.3(c)). These issues fall outside the scope of what is permitted within the four corners of section 14, given the record before this Court.

[58] The Applicant says at paragraph 53 of her memorandum of fact and law that “despite Amazon’s own claim that the Applicant is not authorized to access the account because it cannot verify her identity, the Privacy Officer [of Amazon] suggested that the Applicant is still somehow authorized to reset the password”. That is another issue that can be addressed and dealt with quickly. With respect, this is not what the Respondent asserted. There was no granting of an authorization. The use of a password is only the means to an end, that is to gain access. Access to private information is not granted unless authentication can take place. Once a proper authentication has taken place, access is granted. Amazon did not authorize to reset the password. It suggested that this be done in order for access to take place. I would simply remind the parties of the communication by the Respondent’s Privacy Officer of October 12, 2021, to Ms. James. For ease of reference, I reproduce again the whole email message:

> I am writing in response to your letters dated 11/13/2020 and 9/22/2021, in which you request access to personal information associated with the email address REDACTED. First, I want to apologize for any confusion, frustration or difficulty that you have experienced. I understand that you had a very negative experience and I want to assure you that we have taken your feedback into account and are deep-diving ways to improve the customer experience associated with information requests.
>
> Unfortunately, we cannot grant you access to the information you have requested because we cannot verify your identity. On calls with your customer service representatives, you were unable to verify then name of the account holder and the mailing or billing address associated with the account. When we spoke on 9/29, you indicated that you did not wish to provide additional information, did not want a customer service representative to call you back, and did not want to proceed with our self-service options. If you change your mind, I am happy to assist you.
>
> For reference, you can change the password to your account using your email address by following the instructions here. Once your password is changed and you can login to your account, you can go to our Request Your Personal Information help page and follow the instructions to have a copy of your personal information emailed to you. You can also request the closure of your account and the deletion of your personal information.
>
> (Applicant's record, p 64.)

Assistance was available. The Applicant chose to not use it.

[59] It is worth mentioning that the Privacy Commissioner, in his Report of Findings on February 15, 2022, specifically found that "Amazon reached out to you to determine if it could authenticate the account using alternate means, but did not receive the information it had requested".

V. The Case for the Respondent

[60] Amazon seeks the dismissal of Ms. James' application with costs.

[61] In Amazon's version of events, it acted in accordance with obligations under PIPEDA when it declined to provide Ms. James the information associated with the account in question. It characterizes the main issue before the Court as being one of authentication. That is, Amazon has put security safeguards in place to prevent unauthorized access to accounts. Despite the Applicant's attempts to log into the account, her inability to verify the information that was associated with that account proved to be fatal to her request to access information. At the hearing, counsel for the Respondent articulated this position as follows: "Insistence does not equal authentication".

[62] Amazon raises a preliminary objection to the Court's jurisdiction to entertain the majority of the claims advanced by the Applicant (Respondent Factum, para 13). Amazon's contention is that Ms. James asks the Court to consider new issues that were not contained in the complaint she filed with the Commissioner and therefore falls beyond the scope of what was decided in the Report of Findings. The Respondent relies on the language and interpretation of section 14 of PIPEDA to assert that only matters that are originally complained about, or referred to in the Report of Findings, are subject to an application for judicial review under section 14.

[63] On this basis, Amazon submits that the Court lacks jurisdiction to consider the following "new matters":

A. Amazon's alleged failure to respond to the Applicant's request for information within 30 days (Respondent Factum, para 20);
B. Amazon's alleged breach of Principle 6 of PIPEDA (the Accuracy Principle) (Respondent Factum, para 25);
C. Amazon's alleged use of artificial intelligence and automated decision-making systems (Respondent Factum, para 41).

[64] The Respondent seeks for the Court to decline to respond to the question of whether Amazon failed to respond to the Applicant's request within the 30-day requirement (Respondent Factum, para 20). It relies on the language of section 14 of PIPEDA to argue that the Applicant seeks to expand the scope of the proceedings by including this issue since it was not complained of or referred to in the Report of Findings. The Respondent also relies on para 31 of *Miglialo*, where the Court noted, "The Court does not have jurisdiction if what it raised does not fall within the four corners of section 14".

[65] The Respondent similarly challenges the Court's jurisdiction to consider Amazon's alleged non-compliance with Principle 6 of PIPEDA (Respondent Factum, para 25). In her original complaint, Ms. James did not invoke the Accuracy Principle. As such, the Report of Findings did not address it, and therefore the Court should decline its jurisdiction over the issue.

[66] Finally, Amazon argues that any allegations regarding Amazon's supposed use of artificial intelligence and automated decision-making systems falls squarely outside of the scope of what is reviewable under section 14 (Respondent Factum, paras 41-42).

[67] Should the Court rule that it has jurisdiction to consider these three issues, Amazon makes submissions in the alternative that none of its actions gave rise to a breach of PIPEDA. For each issue, the Respondent argues that Ms. James has failed to discharge her burden of showing that Amazon violated PIPEDA on a balance of probabilities. In particular, she has not satisfied the requisite standard of proof by presenting "sufficiently clear, convincing and cogent evidence" of a breach (Respondent Factum, para 14).

[68] On the first issue, i.e. Amazon's alleged failure to respond to the Applicant's request within 30 days, the Respondent claims that the provision for delay under section 8(3) of PIPEDA or clause 4.9.4 has yet to be triggered (Respondent Factum, para 24). Amazon's repeated attempts to authenticate the Applicant's identity ought to be considered as a prerequisite to proceeding with the access request process (Respondent Factum, para 23).

[69] On the second issue, that is, whether Amazon breached the Accuracy Principle under clause 4.6, Amazon reiterates that there is no evidence on the record that might substantiate a claim that the authentication issues arise as a result of "erroneous" or "faulty" data or the existence of a "privacy breach" (Respondent Factum, para 29). Nor did the Applicant attempt to correct or modify personal information associated with the account (Respondent Factum, para 32). Amazon submits that the authentication of an account holder is a precondition to the modification or correction of that individual's personal information (Respondent Factum, para 30). Therefore and in any event, even if the Applicant had requested to make a correction to the account, she would first have to authenticate herself as the account holder (Respondent Factum, para 32).

[70] Finally, regarding Amazon's alleged reliance on artificial intelligence and automated decision-making, Amazon claims that any adjudication of the issue is ill-founded given the lack of evidence adduced on the topic in this matter (Respondent Factum, paras 43, 47). I have already disposed of these arguments and there is no need to come back to these.

[71] The Respondent does not challenge the Court's jurisdiction to consider the Applicant's claim under clause 4.9.1. This claim pertains to Amazon's decision to refuse to give Ms. James access to information associated with the Account (Respondent Factum, para 26). However, Amazon argues that Ms. James' claim cannot succeed on this ground because it properly saw fit to require an individual to provide sufficient information to authenticate his or her identity (para 37):

4.9.2	**4.9.2**
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. The information provided shall only be used for this purpose.	Une organisation peut exiger que la personne concernée lui fournisse suffisamment de renseignements pour qu'il lui soit possible de la renseigner sur l'existence, l'utilisation et la communication de renseignements personnels. L'information ainsi fournie doit servir à cette seule fin.

[72] In broad terms, Amazon's view is that an individual's right to access their personal information must be balanced against an organization's legal obligation to protect that information from unlawful access and use. The Respondent claims that it has fulfilled its obligations to protect personal information against unauthorized access, use or modification pursuant to Principle 7 (Respondent Factum, para 37).

[73] Amazon relies on two PIPEDA Case Summaries where the Privacy Commissioner found that an organization requiring identification prior to responding to request to access to personal information does not contravene Principle 9 (see: PIPEDA Case Summary #334, *Bank requires piece of identification before responding to request to access to personal information*, 2006 CanLII 29536; PIPEDA Case Summary #324, *Consumer complains about requirement to provide identification in order to obtain credit report*, 2006 CanLII 18528). Amazon notes that since the Applicant has yet to confirm her identity as the one with the right access to the personal information associated with the account, its continued refusal is reasonable pursuant to clause 4.9.2.

[74] In any event, Amazon asserts that the Applicant's claim that it breached clause 4.9.1 is unfounded (Respondent Factum, para 35). In particular, Amazon argues that there is insufficient evidence on the record to support the Applicant's claim that it denied the Applicant access to the account "despite knowing" that she was the account holder (Respondent Factum, para 36). To the contrary, Amazon points to the various interactions between Ms. James and Amazon representatives as demonstrating Amazon's willingness to pursue additional steps to authenticate Ms. James.

VI. Report of Findings

[75] On February 15, 2022, the Commissioner issued a Report of Findings where is confirmed the earlier decision to discontinue the investigation into the Applicant's complaint (Applicant's record, p 10).

[76] Contrary to the Applicant's allegation that Amazon wrongfully denied her access to information related to her account, the Commissioner found that Amazon had provided a "fair and reasonable" response to the complaint (Applicant's record, p 11). The three most salient paragraphs read as follows:

> During the course of our investigation, we learned that Amazon had denied your access requests because it could not verify your identity. Specifically, and as Amazon advised in its email to you dated 12 October 2021, the account holder name, mailing and billing addresses you provided to Amazon were not a match to the information it had on file for the account in question. Following our Office's intervention, Amazon reached out to you to determine if it could authenticate the account using alternate means, but did not receive the information it had requested.
>
> Amazon also advised our Office that there were no indicia of an account takeover and that you could reset your password using the self-serve option. You indicated to our Office to our Office [sic] that you did not want to reset your password using this method because you did not want to accept Amazon's Terms of Service. While it is your decision whether or not to accept an organization's Terms of Service, Amazon's refusal to provide access to personal information when it was unable to verify identity, is in our view, consistent with its obligations under PIPEDA.
>
> Principle 4.7 of PIPEDA provides that personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 further requires that the safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. As such, we are of the view that Amazon provided you with a fair and reasonable response to your access request when it could not verify your identity.

[77] The Report of Findings, which confirms the Privacy Commissioner's decision not to investigate further the complaint made on November 2, 2020, zeroes in on the inability for Amazon to verify the identity of the person seeking access to personal information. The Report finds that Amazon's refusal was justified.

[78] The Privacy Commissioner adds that PIPEDA requires that personal information be protected by security safeguards commensurate with the sensitivity of the information (Principle 7). The Report of Findings refers specifically to clause 4.7.1 which reads:

4.7.1	**4.7.1**
The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.	Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

[My emphasis.]

As can be seen, the security safeguards shall protect against various misuses going all the way to protecting against modifications of the personal information. It is mandatory. Indeed, clause 4.7.3(c) provides in particular that the "methods of protection should include technological measures, for example, the use of passwords and encryption". [My emphasis.]

[79] The Applicant insisted, on numerous occasions during the hearing of this case, that the use of a password was not the issue. It is rather that Amazon had an obligation to provide her the personal information associated with her account. Evidently, Amazon also has the obligation under PIPEDA to safeguard the personal information. The *Interpretation Act*, RSC 1985, c I-21, is unequivocal at its section 11: "The expression "shall" is to be construed as imperative and the expression "may" as permissive". To put it plainly, the law makes an obligation for organizations

to safeguard personal information and one of the tools for that purpose specifically referenced is the use of passwords. The requirement for a password is relevant to the complaint made by Ms. James.

[80] The Commissioner refers to the reasons for denying access as being that the Respondent could not verify the identity. Referring directly to the last email from Amazon, that of October 12, 2021, the Commissioner reports that the Respondent advised that "the account holder name, mailing and billing address you provided to Amazon were not a match to the information it had on file for the account in question". The Report states that "Amazon also advised our Office that there were no indicia of an account takeover".

[81] The Commissioner notes that, following an intervention by the Office of the Privacy Commissioner, the Respondent reached out to the Applicant "to determine if it could authenticate the account using alternative means, but did not receive the information it had requested".

[82] Resetting the password was not an option the Applicant wished to pursue "because you did not want to accept Amazon's Terms of Service". The Commissioner goes on to acknowledge that the Applicant can refuse to accept the Terms, but it remains that Amazon's refusal to provide access when unable to verify identity is consistent with obligations under PIPEDA.

[83] The Commissioner remarks that personal information must be protected, in accordance with Principle 7, against loss or theft, unauthorized access, disclosure, copying, use or

modification. The Commissioner then states that "(a)s such, we are of the view that Amazon provided you with a fair and reasonable response to your access request when it could not verify your identity".

[84] In application of paragraph 12.2(1)(c) of the PIPEDA, the investigation of the complaint was discontinued.

VII. Analysis

[85] This case turns, first and foremost, on the allegation of violation of Principle 9, which requires that someone be given access to her personal information. However, in order to provide that access, PIPEDA requires that the individual supply "sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information" (clause 4.9.2). That is in conformity with the purpose of the legislation said to be "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 information in a manner that recognizes the right of privacy of individuals with respect to their personal information…" (section 3 of PIPEDA). Not only Parliament did not ignore the existence of new technology, but it created legislation to protect privacy in view of the new technology. It is therefore not surprising that is embraced at clause 4.7.3(c) the use of passwords and encryption in order to protect privacy.

[86] The Applicant has not shown how the Respondent can be said to have violated her right to access unless and until it has been possible to verify that she can have access that the private

information held by the Respondent. It seems to me to be unequivocal that the Respondent was under an obligation to protect that information: that is the very purpose of the PIPEDA. Principle 9 provides specifically that access can be denied when the information cannot be disclosed for legal and security reasons. Principle 7 requires that personal information be safeguarded: that is a legal obligation, the violation of which could result in a hearing before this Court pursuant to section 14 of PIPEDA. The importance of protecting personal information is underscored by clause 4.9.2 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". The Respondent could be faulted for disclosing personal information without the appropriate authorization. It was justified in refusing to give access to personal information without being able to authenticate the identity of the requester in the circumstances of this case.

[87] Ms. James argues that the reason for her inability to gain access to what she considers to be her personal information is that there is some inaccuracy such that Principle 6 is engaged and violated.

[88] The Respondent contends that the Court does not have the jurisdiction to consider compliance with Principle 6 because it falls outside the scope of the complaint (Applicant's record, pp 32-33) made and the Commissioner's Report of Findings, and, accordingly, outside the scope of section 14 of the PIPEDA. A close examination of the complaint would tend to confirm the Respondent's argument. Principle 6 was never raised. Ms. James wrote in her complaint to the Privacy Commissioner that "Amazon.com Inc. is refusing to provide me with

access to my personal information and refuses to provide receipts of online purchases requested in writing on 2 September 2020". The longer explanation found in the complaint does not shed a different light on the issue. The matter raised with the Privacy Commissioner was limited to access. The Report of Findings of the Commissioner does not either refer to Principle 6 as being an issue.

[89] But there is more. As noted before, the record before the Court is devoid of any evidence that could give the issue of accuracy an air of reality. It is more in the nature of the beginning of an attempt by the Applicant at an explanation for the inability to authenticate her identity. We are far from the standard of clear, convincing and cogent evidence in support of the application. Finally, I was concerned that Principle 6 may not be applicable, as clause 4.6.1 provides that "(i)nformation shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual". The purpose of Principle 6 may not be that which is proposed by the Applicant. It may be that the personal information that is disclosed must be accurate in view of the damage inaccurate personal information may cause if disclosed in that inaccurate state. However, as this precise issue was not raised, the Court does not have the benefit of the views of the parties and refrains from considering the issue any further.

[90] Ms. James raised the issue of timeliness of the response. The Respondent argued again that the Court lacks jurisdiction because it was not part of the complaint to the Privacy Commissioner. It is true that in the complaint itself there was no mention of the requirement to

respond within a period of time. However, as pointed out by Ms. James, the complaint included appended documents some of which speak of a timely response.

[91] At any rate, there was a response given by the Respondent in a timely fashion. But the Respondent was not able to grant access without proper authentication. The Respondent brought to the Court's attention PIPEDA Case Summary #334 (2006 CanLII 29536). Not only did the Assistant Commissioner of Privacy find that it was reasonable to require to identify oneself before an access request is processed, but it was found that the 30-day timeframe began once the request is complete. The Court agrees that the sufficient information to permit the disclosure of personal information (clause 4.9.2) must be the starting point for the calculation of the "thirty days after receipt of the request" of section 8(3) of PIPEDA. As I pointed out during the hearing of this case, there may be circumstances where an organization may require that the "sufficient information" of clause 4.9.2 be so extensive that the 30-day period is abused. Such is not the situation in the instant case. Accordingly, there is no violation of the timeliness requirement.

[92] As already found, the arguments offered by the Applicant concerning the alleged use by Amazon of artificial intelligence and automated decision-making systems fall outside the scope of what is permitted under section 14 of PIPEDA.

[93] It follows that the application must be dismissed because the principles of Access and Accuracy have not been proven to have been violated on this record, nor is the requirement for timeliness.

[94] I offer one final observation. Amazon, on October 12, 2021, offered to assist in verifying the Applicant's identity (Applicant's record, p 64). That offer was noted in the Report of Findings of the Privacy Commissioner. It seems that Ms. James refused to reset her password because she did not want to accept Amazon's Terms of Service. I have reviewed the Terms of Service which were made part of the Applicant's record (pp 131 to 139), and in particular the highlighted portions as presented by the Applicant. It seemed to me that there is no material difference between the updated version of what is presented as "Amazon.ca Privacy Notice (last updated May 14, 2021)" which presumably would apply if the password were to be reset in October 2021, compared to the conditions of use, notices and revisions in the preceding Notice (last updated May 18, 2020).

[95] It is less than apparent what the issue related to the Terms of Service may be. Be that as it may, the October 12, 2021 email not only offers assistance, but the point is made clearly that once the Applicant has retrieved her personal information, assuming that her identity has been authenticated, she "can also request the closure of your account and the deletion of your personal information". In that context, the issue of the Terms of Service may be a red herring. That may provide further support for the conclusion reached by the Privacy Commissioner that "(w)hile it is your decision whether or not to accept an organization's Terms of Service, Amazon's refusal to provide access to personal information where it was unable to verify identity is, in our view, consistent with its obligation under PIPEDA". Put differently, no one suggests that the Applicant should carry on a relationship with the Respondent, when the Terms of Service may be an issue, beyond gaining access to her personal information if that is her wish.

VIII. Conclusion

[96] It is unfortunate that a matter that could, and probably should, have been resolved with an appropriate dialogue between the Applicant and the Respondent ends up before this Court. The PIPEDA's purpose is to protect against inappropriate disclosure of personal information. There is no reason to insist further on the importance of privacy. Yet, it is rather unusual that a person who seeks access to what she alleges is her own personal information would be denied if in fact that personal information is hers. This case leaves the issue without an explanation: there is simply no clarity as to what has taken place. Why, if the Applicant's personal information is held by the Respondent, has she not been able to gain access? What prevents the resolution of this matter, one way or the other? Would a more open dialogue have averted ending up in court?

[97] It is obviously not for this Court to seek to answer the question. Its jurisdiction is limited to hearing, on the basis of the record presented to it, the case in respect of any matter in respect of which the complaint before the Privacy Commissioner was made or that is referred to in the Report of Findings. The Applicant made allegations and the Court adjudicates on that basis.

[98] In this case, the Applicant claimed a violation of Principle 6, about the accuracy of the information held by Amazon, and Principle 9, about her inability to have access to that information. She also argued that she did not have a response within the time allocated by the legislation.

[99] As the Court explained, the burden on the Applicant to show a violation of principles 6 and 9, more fully articulated in clauses 4.6 and 4.9, has not been discharged. As for a response within the allocated period of time, the record shows that there was a response within the allocated period of time, but the Respondent had to protect the personal information from disclosure, and the Applicant was "required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information" (clause 4.9.2). Access was denied for valid reasons. It follows that it cannot be found that the response was not supplied within the time limit. It requires that a proper request for the personal information be made for the clock to be ticking.

[100] Ms. James speculates when she contends that the failure to authenticate is because of inaccurate information held by Amazon. The Applicant assumed that the difficulty stemmed from information held by the Respondent which would have been modified (the Accuracy Principle). There is no basis in the record to support that assumption.

[101] As for the suggestion made by the Applicant that artificial intelligence (and the use of automated decision-making systems) had something to do with the alleged violation of principles 6 and 9, it is difficult to see how it fits in this case within the confines of section 14 of PIPEDA. This suggestion was never part of the complaint made on the Report of Findings because it was not made. Moreover, in the case at hand, there is a complete lack of evidence; on the contrary, the evidence is that the Applicant was in contact with representatives of the Respondent, including a human Privacy Officer. The Applicant's suggestion is of no assistance in resolving the issue.

[102] The obvious frustration of the Applicant, but also that of the Respondent, is understandable. One wants to gain access to what she claims is her personal information, only to be told that access must be denied for lack of authentication because of the requirements of PIPEDA. The other seeks to assist, by providing an opportunity to change the password under its supervision and assistance, without any taker. The Respondent has acted within the confines of the PIPEDA. It remains that there was, and continues to be, a stalemate.

[103] This obviously leaves the issue unresolved. The Court invites the parties to resume their dialogue to find a solution in order to ascertain, with a measure of certainty, whether the Applicant should have access to the personal information she claims is in the possession of the Respondent. Alternate means of authentication may be an avenue to explore if the resetting of a password, under supervision and with the assistance of the Respondent, proves to be a dead end.

[104] Both parties sought costs for these proceedings. This is not a case for costs.

[105] It follows that the application under section 14 of PIPEDA must be dismissed without costs.

JUDGMENT in T-1335-22

THIS COURT'S JUDGMENT is:

1. The application under section 14 of the *Personal Information Protection and Electronic Documents Act* is dismissed.

2. No costs are awarded.

"Yvan Roy"
Judge

ANNEX A

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 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.	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 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.

4.9.2

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. The information provided shall only be used for this purpose.

4.9.2

Une organisation peut exiger que la personne concernée lui fournisse suffisamment de renseignements pour qu'il lui soit possible de la renseigner sur l'existence, l'utilisation et la communication de renseignements personnels. L'information ainsi fournie doit servir à cette seule fin.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.3

L’organisation qui fournit le relevé des tiers à qui elle a communiqué des renseignements personnels au sujet d’une personne devrait être la plus précise possible. S’il lui est impossible de fournir une liste des organisations à qui elle a effectivement communiqué des renseignements au sujet d’une personne, l’organisation doit fournir une liste des organisations à qui elle pourrait avoir communiqué de tels renseignements.

4.9.4

An organization shall respond to an individual’s request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.4

Une organisation qui reçoit une demande de communication de renseignements doit répondre dans un délai raisonnable et ne peut exiger, pour ce faire, que des droits minimes. Les renseignements demandés doivent être fournis sous une forme généralement compréhensible. Par exemple, l’organisation qui se sert d’abréviations ou de codes pour l’enregistrement des renseignements doit fournir les explications nécessaires.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of

4.9.5

Lorsqu’une personne démontre que des renseignements personnels sont inexacts ou incomplets, l’organisation doit apporter les modifications nécessaires à ces renseignements. Selon la

the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

nature des renseignements qui font l'objet de la contestation, l'organisation doit corriger, supprimer ou ajouter des renseignements. S'il y a lieu, l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.9.6

Lorsqu'une contestation n'est pas réglée à la satisfaction de la personne concernée, l'organisation prend note de l'objet de la contestation. S'il y a lieu, les tierces parties ayant accès à l'information en question doivent être informées du fait que la contestation n'a pas été réglée.

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-1335-22
STYLE OF CAUSE:	TAMARA JAMES v AMAZON.COM.CA, INC.
PLACE OF HEARING:	MONTRÉAL, QUEBEC
DATE OF HEARING:	JANUARY 18, 2023
JUDGMENT AND REASONS:	ROY J.
DATED:	FEBRUARY 3, 2023

APPEARANCES:

Tamara James	FOR THE APPLICANT (ON HER OWN BEHALF)
Alexandra Quigley	FOR THE RESPONDENT

SOLICITORS OF RECORD:

Dentons Canada, S.E.N.C.R.L. Montréal, Quebec	FOR THE RESPONDENT