ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER P2020-07

December 9, 2020

HI LINE FARM EQUIPMENT LTD

Case File Number 005742

Office URL: www.oipc.ab.ca

Summary: The Complainant complained to the Commissioner that his former employer Hi Line Farm Equipment Ltd (the Organization) had collected, used, and disclosed his personal information in contravention of PIPA when it accessed texts and emails he had made on his work-issued iPhone and produced them in litigation between the Complainant and the Organization.

The evidence established that the Organization had provided the iPhone to the Complainant for work purposes. The Complainant did not return the iPhone when his employment ended, but continued to use the iPhone after changing the SIM card and obtaining a new telephone number for the iPhone. The Apple ID for the iPhone remained the Organization's, as did the iCloud account. There was no evidence that the Organization authorized the Complainant to keep the iPhone and continue using its Apple ID or iCloud account.

The Adjudicator determined that the Complainant had not adduced sufficient evidence to meet the evidential burden in the inquiry. A complainant has the burden of pointing to evidence that an organization has collected, used, and disclosed personal information in the circumstances the complainant alleges. In this case, there was no evidence to establish that the Organization had done anything other than to access its iCloud account in order to prepare for litigation. PIPA authorizes organizations to collect and use personal information without the consent of the individual the information is about when the organization's purpose for collection is to prepare for litigation.

Statutes Cited: AB: *Personal Information Protection Act*, S.A. 2003, c P-6.5 ss. 1, 7, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

Authorities Cited: AB: Orders P2006-004, P2006-008, P2008-010, P2012-08, P2012-09, F2019-05

Cases Cited: AB: *Edmonton (City) v Alberta (Information and Privacy Commissioner)*, 2016 ABCA 110 (CanLII); *District of Houston v Canadian Union of Public Employees, Local 2086*, 2019 CanLII 104260 (BC LA); *Rancourt-Cairns v. The Saint Croix Printing and Publishing Company Ltd.* 2018 NBQB 130 (CanLII); *Aon Benfield Canada ULC v. Vazir*, 2018 ONSC 4529 (CanLII)

I. BACKGROUND

[para 1] On January 22, 2016, the Complainant's employment with Hi Line Farm Equipment Ltd (the Organization) terminated. He replaced the SIM card on the iPhone the Organization had provided for performing work duties and obtained a new telephone number for the iPhone. He continued to use the iPhone for personal and business matters.

[para 2] On April 5, 2017, the Complainant complained to the Commissioner that the Organization had "hacked" his iPhone. In support of his position, he pointed to texts and emails he had sent and received using the iPhone that the Organization had then produced in litigation.

[para 3] The Commissioner authorized a senior information and privacy manager to investigate and attempt to mediate a settlement of the matter. At the conclusion of this process, the Complainant requested an inquiry. He complained that the Organization had not warned him that information saved to the Organization's iCloud account could be accessed by the Organization. He stated:

> When [the Complainant] entered his new SIM card and number, he also connected to the iCloud account he had used previously. He did not know and was not informed that Hi Line could continue to access that iCloud account and collect information on his phone.
>
> [The Complainant] filed a lawsuit against Hi Line for issues related to his employment with them. On March 24, 2017 a representative of Hi Line endorsed an Affidavit of Records including text messages, photos, and location data from both during [the Complainant's] employment with Hi Line and after.
>
> [The Complainant] lost the phone provided by Hi Line. On May 10, 2017 [The Complainant] got a new phone, and a new sim card. He is now using a different iCloud account.

[para 4] The Commissioner agreed to conduct an inquiry and delegated her authority to conduct it to me. After I reviewed the complaint and the request for inquiry, I decided that I would ask questions of the Complainant before hearing from the Organization. On May 12, 2020, I asked the Complainant the following questions:

With regard to the Apple ID used to activate the iPhone, was it the Complainant's Apple ID or that of the Organization that was used?

To what extent was the Complainant authorized to use the iPhone for personal purposes as opposed to business purposes?

Who was the owner of the iPhone?

When can it be said that the Organization collected the Complainant's personal information? At the time it became accessible via the Cloud or at the time the Organization accessed it? When does the Complainant believe the Organization accessed the information?

Why does the Complainant believe that the Organization was actively monitoring or gathering information from his texts and emails as he made them? Is there an organizational practice of which he is aware, or is there some other evidence that led to this conclusion?

[para 5] The Complainant responded:

1) With regard to the Apple ID used to activate the iPhone, was it the Apple ID or that of the Organization that was used?

The Apple ID used to activate the iPhone was set up and held by the Organization and the ID and password information were provided to the Complainant. The Complainant did not have the Apple ID prior to employment with the organization.

2) To what extent was the Complainant authorized to use the iPhone for personal purposes as opposed to business purposes?

The Complainant was authorized to use the iPhone for personal use as well as for business purposes, with no specific limitations. Given that the Complainant's role was direct to consumer sales, he could be making business calls at any time of the day. It therefore made sense that his business and personal cell phone would be the same, and both parties agreed to and were aware of this.

3) Who was the owner of the iPhone?

The Organization purchased the iPhone and was the owner of it up until the termination of the Complainant's employment with the Organization on January 22, 2016, after which the Complainant was the owner of the phone. On February 22, 2016 the Complainant purchased a new sim card for the iPhone and got a new phone number for the phone as well. The Complainant did not set up a new iCloud account until May of 2017.

4) When can it be said that the Organization collected the Complainant's personal information? At the time it became accessible via the Cloud, or at the time the Organization accessed it? When does the Complainant believe the Organization accessed the information?

The Organization had access to the information on the Complainant's iPhone, including but not limited to personal texts, photos, and the phone's location, at all times. The Organization set up the Complainant's iCloud and backup system, and had access to the iCloud and the backups at all times, including after the Complainant no longer worked for the Organization, and after the Complainant had purchased a new sim card and phone number for the iPhone.

The Organization also had the ability to access the Complainant's iCloud and phone

backups even if the Complainant changed the password, as the Organization could access the password information through the Complainant's email address.

The Organization should be considered to have collected the information as soon as they had access to it. As stated previously, the Organization purchased the iPhone and set up the iCloud account, meaning that as far as Apple is considered, the Organization is the owner of the information on the iCloud account. If either Apple or the Organization did not believe that the Organization was the owner of this account, then both of them have responsibilities to justify the reason for the collection of the information, as is required by section 13 and section 13.1 of the *Personal Information and Privacy Act.*

The earliest date of the text messages accessed by the Organization was September 1, 2015, so we know that the Organization had access to information dating from at least that time. The Complainant does not have specific evidence of the Organization accessing the Complainant's information prior to this date.

Regardless of when the Organization accessed the information on the iCloud account, the Complainant submits that as soon as the Organization had access to the information, it should be considered to have collected it. This is consistent with the definition in section 5 of the *Personal Information and Privacy Act,* which states "An organization is responsible for personal information that is in its custody or under its control." The Organization had the information on the iCloud under its control at all relevant times. The holding of that information in an iCloud account to which the Organization had access is no different than the Organization storing that information in paper form at an off-site storage unit - if they have access to and control of the information at all times, they must be considered to have collected it.

At no time did the Complainant authorize the Organization to hold this information. The Complainant was not aware of the information being collected by the Organization, and it is not reasonable for the Organization to collect the Complainant's personal correspondence, photos, and location for any purpose.

5) Why does the Complainant believe that the Organization was actively monitoring or gathering information from his texts and emails as he made them? Is there an organization practice of which he is aware, or is there some other evidence that led to this conclusion?

The Complainant does not have any specific evidence that the Organization was monitoring the iCloud account on a regular basis, or that there was a specific policy where the Organization would do so.

[para 6] After I reviewed the Complainant's answers, I decided to complete the inquiry without hearing from the Organization.

II. ISSUES

ISSUE A: Did the Organization collect the Complainant's "personal information" as that term is defined in PIPA?

ISSUE B: If so, did the Organization collect, the information contrary to, or in compliance with, section 7(1) of PIPA (no collection, use or disclosure without either authorization or consent)?

ISSUE C: Did the Organization collect, use or disclose the information contrary to, or in accordance with, sections 11(1), 16(1) and 19(1) of PIPA (collection, use and/or disclosure for purposes that are reasonable)?

ISSUE D: Did the Organization collect, use or disclose the information contrary to, or in accordance with, sections 11(2), 16(2) and 19(2) of PIPA (collection, use and/or disclosure to the extent reasonable for meeting the purposes)?

III. DISCUSSION OF ISSUES

ISSUE A: Did the Organization collect the Complainant's "personal information" as that term is defined in PIPA?

[para 7] Personal information is defined by section 1(1)(k) of PIPA as "information about an identifiable individual". This definition has been interpreted in past orders. For example, in Order P2012-09, the Adjudicator commented that not all the information in an individual's personnel file is about the individual, such that it could be said to be "personal information". She said:

> As noted, some of the records provided to the Applicant contain no information at all about her; the fact that these records may have been located in the Applicant's personnel file does not necessarily mean that they contain her personal information under PIPA. Even the records that contain the Applicant's name are not subject to an access request under PIPA where they contain no "personal dimension." For example, as the Applicant's position with the Organization required certain safety training, some of the records provided to the Applicant by the Organization were training materials (for example, pages 622-649 consist of an operator training manual). The Organization's training manuals cannot be characterized as the Applicant's personal information. This is the case even in the instances wherein the training materials included quizzes with the Applicant's answers, as well as her signature affirming that she had read the materials, as there is no personal dimension to the information in these records. I make the same finding with respect to copies of organization-wide policy memos and records of work-related meetings and attendance at those meetings.
>
> Shift-related information, such as voluntary leave forms (signed when an employee voluntarily leaves early due to lack of work), and shift change forms (signed by two employees switching shifts) is also not the Applicant's personal information. A record showing that an employee worked on a particular day does not reveal information that has a personal dimension such that it is personal information about that employee. Although these records show that the Applicant left a shift early or changed a scheduled shift, in my view, this information is better characterized as information about the Applicant's work or position, rather than about the Applicant. The same is true regarding the names of coworkers on the shift change forms and other shift-related records (daily schedules on pages 238, 1095 and 1096, and a letter denying a request to change shifts on page 411). (In saying this I acknowledge that there may be other situations in which shift-related information has a personal dimension).

[para 8] In Order P2006-004, former Commissioner Work commented that most information in legal files will not be personal information within the terms of PIPA. He said:

> The Act defines "personal information" as "information about an identifiable individual". In my view, "about" in the context of this phrase is a highly significant restrictive modifier. "About an

> applicant" is a much narrower idea than "related to an [applicant]". Information that is generated or collected in consequence of a complaint or some other action on the part of or associated with an applicant - and that is therefore connected to them in some way - is not necessarily "about" that person. [My emphasis] In this case, only a part of the information that the [applicant] asked for was information "about" him. Had he relied on PIPA to obtain information, he would not have received much of the information that was made available to him under the *Legal Profession Act* and the Rules created thereunder, or pursuant to the requirements of fairness.
>
> […]
>
> I do not need to decide for the purpose of this inquiry precisely which parts of the information in the documents collected or created for the purpose of the complaint proceedings were "personal information" of the [applicant], as that term is to be understood in PIPA. It is sufficient to say that there is a great deal of information in the documents that is not the [applicant's] personal information even though it was generated in consequence of his complaints. The latter includes information about the persons about whom he complained and their dealings with the [applicant], information about other third parties and their dealings with the [applicant], descriptions of various events and transactions, and correspondence and memos related to the handling of the complaints and other aspects of the complaint process. As well, the fact the [applicant] was the author of documents does not necessarily mean that the documents so authored were his personal information**.**

[para 9] The foregoing orders clarify that information must be "about" an identifiable individual before it will be considered "personal information" within the terms of PIPA. Information that is merely related to an individual or generated by an individual is not "personal information". Moreover, information about an individual acting in a representative capacity is also not "personal information", as I noted in Order P2012-08. In that order, I said:

> If information about an individual acting solely in a commercial capacity, or solely in a capacity as a representative of an organization, is to be interpreted as personal information, then this interpretation would have the effect of protecting information rights of some, but not all, organizations. An organization collecting the business information of sole proprietors or single shareholder corporations would arguably be required to comply with PIPA when they do so, even though it would not be necessary to do so in the case of a larger organization. Such a result would appear to be entirely arbitrary, given that both small and large organizations may conduct the same business and be required to furnish the same kinds of information to other organizations. In my view, the better approach is to consider that information that is about an individual acting solely in the individual's capacity as a representative of an organization, or in a commercial capacity is not personal information for the purposes of section 1(1)(k).

Past orders of this office have held that information about the representative of an organization will be personal information if it has a personal dimension, such as when the information is about the representative acting as an individual citizen or has personal consequences for the representative in the representative's personal capacity. In *Edmonton (City) v Alberta (Information and Privacy Commissioner)*, 2016 ABCA 110 (CanLII), the Alberta Court of Appeal considered this approach, under both the FOIP Act, and PIPA, to be reasonable. The Court said:

> In general terms, there is some universality to the conclusion in *Leon's Furniture* that personal information has to be essentially "about a person", and not "about an object", even though most objects or properties have some relationship with persons. As the adjudicator recognized, this

> concept underlies the definitions in both the *FOIPP Act* and the *Personal Information Protection Act.* It was, however, reasonable for the adjudicator to observe that the line between the two is imprecise. Where the information related to property, but also had a "personal dimension", it might sometimes properly be characterized as "personal information". In this case, the essence of the request was for complaints and opinions expressed about Ms. McCloskey. The adjudicator's conclusion (at paras. 49-51) that this type of request was "personal", relating directly as it did to the conduct of the citizen, was one that was available on the facts and the law.

[para 10] Of the information that is the subject of the complaint, I note that the majority is not personal information about the Complainant. Rather, most of the information is either about the Complainant acting in a representative capacity, when the information could be said to be "about" him, or is information about other people, or is simply information associated with the Complainant, rather than being about him. For example, photographs of guns that appear in the records are not "about" the Applicant. Such information is not subject to PIPA and is outside my jurisdiction to address. However, I accept that the information appearing in the Organization's affidavit of records regarding the Complainant's views about a family event is his personal information, as well as his views about family members and information about his health. When I refer to the Complainant's personal information in this order, I am referring only to information of this kind.

[para 11] As I find that some of the information accessed from iCloud is the Complainant's personal information, I conclude that the Organization accessed the Complainant's personal information.

ISSUE B: If so, did the Organization collect, the information contrary to, or in compliance with, section 7(1) of PIPA (no collection, use or disclosure without either authorization or consent)?

[para 12] Section 7 of PIPA imposes an obligation on an organization to obtain consent prior to collecting, using, or disclosing personal information. The relevant provisions state:

> *7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,*
>
> *(a) collect that information unless the individual consents to the collection of that information,*
>
> *(b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source […]*

[para 13] Section 7(1)(a) requires an organization to obtain consent prior to collecting personal information, except in the situation where PIPA permits collection without consent. Section 7(1)(b) prohibits an organization from collecting personal information from a source other than the individual without consent, unless a provision of PIPA authorizes doing so. As there is no question of the Complainant having consented

to the collection of his personal information in this case, the question is whether a provision of PIPA authorized the Organization to collect his personal information in the circumstances that it did.

[para 14] Section 14 of PIPA sets out an exhaustive list of circumstances in which an Organization may collect personal information without consent. It states, in part:

> *14 An organization may collect personal information about an individual without the consent of that individual but only if one or more of the following are applicable:*
>
> *[…]*
>
> *(d) the collection of the information is reasonable for the purposes of an investigation or a legal proceeding […]*

An organization is not required to obtain the consent of an individual, or to provide notice, when it collects personal information that it is reasonable for the purpose of legal proceedings.

[para 15] The Complainant asserts that the iPhone belonged to the Organization and was provided to him for the purpose of performing his duties with the Organization. However, he then asserts that he was the "owner" of the iPhone from the date of the termination of his employment until the date he "lost" the iPhone in May of 2017, without explanation as to how ownership of the iPhone changed.

[para 16] It is unclear from the Complainant's evidence how he could be considered the legal owner of the iPhone the Organization provided, particularly as the account by which the Complainant accessed Apple services, such as password, information storage, location, text, email, software, and security services, remained the Organization's. The Complainant did not indicate in his submissions that anyone at the Organization agreed that the iPhone it provided for performing work duties would become his property on the termination of employment, or that he could continue to use the iCloud account. The Complainant acknowledges that the Apple ID on the phone continued to be the Organization's, even after he changed the SIM card on the iPhone.

[para 17] I note, too, that the Complainant acknowledges that he did use the iPhone for performing work duties when he was employed by the Organization. As a result, any information on the iPhone generated by the Complainant while performing those duties, such as information regarding sales or customers in emails or texts, is the property of the Organization, despite the Complainant's appropriation of the iPhone. In addition, the Organization would have responsibilities under PIPA over any client personal information generated by the iPhone or accessible by it.

[para 18] Despite the Complainant's position that he owned the iPhone as of January 22, 2016, I am unable to accept this position, as the Complainant has not

provided a legal or evidentiary basis to support it. In the absence of any action on the part of the Organization relinquishing its rights to the iPhone to the Complainant on January 22, 2016, I must find that the Organization continued to own the iPhone and that the Complainant unilaterally took possession of it, and continued to use both it and the Apple ID without the Organization's authorization.

[para 19] The Complainant takes the position that the Organization should have warned him that information on the iPhone was accessible by it and that the Organization should be deemed to have collected information as soon as it was accessible on the iPhone. In my view, this is incorrect. There is no basis for this position in PIPA. That an organization has the *ability* to access information via iCloud, or any other means, does not mean that it has actually done so. PIPA does not deem personal information to have been collected, simply because it is accessible to an organization. There is nothing before me to suggest that the Organization collected information generated by the Complainant's use of the iPhone prior to the initiation of legal proceedings. The Complainant concedes this point in answer to my questions, stating:

> The Complainant does not have any specific evidence that the Organization was monitoring the iCloud account on a regular basis, or that there was a specific policy where the Organization would do so.
>
> The date that the Organization made physical copies of the information is immaterial for two reasons. First, as stated above, the Organization had control of the information prior to this date. Secondly, as stated in *Peter Choate* & *Associates Ltd. v. Dahlseide* 2014 ABQB 117 at paragraphs 47-49, section 4(3)(k) should not be interpreted in a manner that should remove the privacy protections intended by the Legislature in *PIPA.* If it is held that the Organization can hold information which it does not have consent to access until such time as it decides to begin a court action, it effectively removes any privacy protection for that information.

[para 20] I acknowledge that the Complainant argues that the Organization had control over the information as he generated it and reasons that the date of collection is immaterial; however, I do not accept this argument. On the evidence before me, there was no reason for the Organization to expect that the Complainant's personal information was accessible to it via iCloud until it began to prepare for litigation and accessed the iCloud account for that reason. Further, there is no evidence that the Organization actually collected the Complainant's personal information from iCloud prior to the onset of litigation.

[para 21] In my view, the situation is similar to that in Order F2019-05 in which a public body had to review files on its computer system to determine which information belonged to a complainant and which belonged to it. The Adjudicator in that case, said:

> In Order F2009-048, I found that reviewing records for the purpose of determining their appropriateness for disclosure is not a 'use' of personal information in those records (see paras. 40-42). In that case, the public body had already collected the personal information for human resources purposes. The public body later reviewed those records to determine their appropriateness for disclosure for a different purpose.
>
> In my view, reviewing records to determine which 'belong' to the Public Body and which do not is not a 'collection' of that information. This outcome is consistent with my findings above

> regarding the scope of 'collection' under Part 2 of the Act; it is also consistent with the scope of 'use', discussed in Order F2009-048.
>
> In other words, JSG did not collect the Complainant's personal information when it reviewed the documents to determine which to give to the Complainant (as they were his personal effects) and which to keep (as work product properly belonging to JSG or AHRC).
>
> That said, I find that JSG *did* collect the Complainant's personal information when it decided to retain the information for its own purposes.

When an individual stores their personal information on an organization's or public body's system without the organization's or public body's knowledge, such as when an employee saves personal files to a hard drive, as was the case in Order F2019-05, *supra*, or an individual saves information to an organization's iCloud account, as is the case here, the organization or public body is not collecting personal information when it sifts through records and information to determine what has been placed on its system.

[para 22] The evidence before me indicates that the Organization collected the Complainant's personal information for the purpose of litigation. Section 14 requires that an organization's purpose for collecting personal information be reasonable for the purposes of litigation, not that every piece of information collected be relevant to litigation. In Order P2008-010, the Director of Adjudication determined that an organization may reasonably collect personal information for the purpose of litigation if the information is of the kind normally considered useful or related to litigation of the kind within contemplation. She said:

> Based on my conclusions in Order P2008-008, I must ask whether, for any such item of information, there is a reasonable likelihood that a legal proceeding will arise relative to which such information will be relevant because the facts or circumstances grounding such a proceeding are likely to happen.
>
> To answer this question, I return to my earlier comments about the work of police officers. As I noted above, the actions taken by police officers in performing their work responsibilities are commonly relevant to the prosecution of offences as well as to their defence. Police work includes not only investigating offences, but also providing evidence about the results of the investigation, as well as, in some circumstances, creating or influencing the creation of relevant information. It is a routine aspect of the work of police officers that information about actions they take in discharging their duties, both relative to a particular prosecution and relative to earlier cases, will be introduced as evidence.
>
> Thus, in my view, if information as to the manner in which a particular police officer has carried out their work exists in the database, it is highly likely that as a matter of course, that information will become relevant to future cases in which they are involved. I do not rule out the possibility that there could be exceptional items of information – for example, such as are unlikely to have any relevance to future events because they arose in highly unique circumstances, or when the information is relative to a particular officer or former officer relative to whom there is no possibility that they may be involved or give evidence in future cases. However, I believe that in the normal course, the happening of future events relative to which offence proceedings would arise, to which such information would be relevant, would be very likely. Similar to what I said in Order P2008-008, it strikes me as not only permissible but prudent to collect relevant information (and to use and disclose it for the same purpose) to provide the basis on which courts can make findings as to credibility, and related issues relating to police conduct, in the future prosecution and defence of charges.

> Based on these conclusions, I find that the collection, use and disclosure of personal information relating to police officers' discharge of their duties, that would be relevant in defences against future legal proceedings that are likely to arise because it is likely the officer will become involved in offence proceedings in the future, is "reasonable for the purpose" of these future proceedings, and falls within the terms of sections 14(d), 17(d) and 20(m). Therefore, as long as this eventuality continues to be reasonably likely, it is, in my view, permissible for the Organization to collect the personal information and to enter it into the database, to use and disclose it as required, as well as to disclose it to other individuals or law firms who reasonably require it for the purpose of defending against offence proceedings.

In the foregoing case, the Director of Adjudication considered that the collection, use, or disclosure of personal information would be reasonable for the purpose of future legal proceedings, if the information is of a type or that is usually collected for proceedings of the kind anticipated.

[para 23] In proceedings arising from termination of employment, the manner in which an employee performed work duties is usually relevant to the cases of both the employer and employee. In some cases, a former employee's handling of the employer's property and confidential information, including after the termination of employment, may also be relevant to an employer organization in litigation. (As discussed above, any business information accessible via iCloud generated by the Complainant prior to his termination, would be the Organization's business information.) Ultimately, the personal information obtained by the Organization may not prove relevant; however, information generated by employees using an employer provided cell phone or computer is often relevant to employment litigation and it is not unreasonable for an Organization to gather such information on the basis that it could be relevant. (See, for example, *District of Houston v Canadian Union of Public Employees, Local 2086*, 2019 CanLII 104260 (BC LA); *Rancourt-Cairns v. The Saint Croix Printing and Publishing Company Ltd.* 2018 NBQB 130 (CanLII) and *Aon Benfield Canada ULC v. Vazir*, 2018 ONSC 4529 (CanLII), in which employees' uses of employer provided cellular phones and computers were relevant to litigation.) The information produced by the Organization is all information that conveys something about the Complainant's handling of the Organization's equipment following the termination of his employment, given that he continued to use the cellphone, rather than return it, even if the substance of the texts and emails is not intended to convey that information.

[para 24] I find that section 14(1)(d) is clear authority for the collection and that the Complainant has not demonstrated that the Organization collected his personal information in circumstances other than those contemplated by section 14(1)(d).

[para 25] A complainant bears the initial burden of adducing or pointing to evidence – "the evidential burden" – to establish his or her personal information was or is being collected in the manner alleged. In Order P2006-008, former Commissioner Work explained the evidential burden for complaints in the following terms:

> This initial burden is what has been termed the "evidential burden". As I have said, it will be up to a complainant to adduce some evidence that personal information has been collected, used or disclosed. A complainant must also adduce some evidence about the manner in which the

> collection, use or disclosure has been or is occurring, in order to raise the issue of whether the collection, use or disclosure is in compliance with the Act.
>
> One of the purposes of the Act is to ensure that organizations collect, use or disclose information for purposes that are reasonable. Accordingly, the threshold for the evidential burden will be low, to allow a matter about an organization's compliance with the Act to be decided in an inquiry. It therefore follows that the Act does not require that a complainant meet a stringent burden of proof as may be required in a court of law, so as to allow a matter about an organization's compliance with the Act to be decided in an inquiry.
>
> In most cases the nature of the complaint will dictate the degree of evidence necessary to establish the basis of the complaint. For example, in Order P2005-001 the Complainant was concerned about disclosure of personal information to websites, employees of the Organization and to third parties. To sustain such a complaint a certain level of specificity in evidence was needed to identify the personal information disclosed and to whom. Usually, this is accomplished by a complainant making a submission detailing the nature of the complaint with supporting evidence.

[para 26] In deciding whether there is sufficient evidence before me for the Complainant to meet the evidential burden, I must consider whether there is evidence before me that could support the Complainant's assertion that the Organization collected the Complainant's personal information in the circumstances he alleges – by accessing the iCloud account without authority.

[para 27] As discussed above, I find that the iCloud account from which the Complainant's personal information was accessed is the Organization's own. I also find that it has not been established that the Organization knew that the Complainant's personal information (those pieces of information I have found to be personal information) would be located in iCloud, given that there is no evidence it authorized the Complainant to continue using the iPhone after the termination of his employment. The only purpose I can reasonably attribute to the Organization in collecting the information, based on the Complainant's evidence, was to prepare for litigation. PIPA authorizes organizations to collect personal information for this purpose without consent.

[para 28] I note that the Complainant also takes the position that the Organization was required by section 13 to provide notice of the collection. Section 13 states, in part:

> *13(1) Before or at the time of collecting personal information about an individual from the individual, [my emphasis] an organization must notify that individual in writing or orally*
>
> *(a) as to the purposes for which the information is collected, and*
>
> *(b) of the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.*

In this case, the Organization did not collect personal information from the Complainant, but reviewed information stored in its iCloud account. As the information was not collected from the Complainant, the Organization was not required to comply with

section 13. In addition, as section 14(1)(d) authorizes the collection without consent, section 12 of PIPA (not reproduced) in turn authorizes indirect collection.

ISSUE C: Did the Organization collect, use or disclose the information contrary to, or in accordance with, sections 11(1), 16(1) and 19(1) of PIPA (collection, use and/or disclosure for purposes that are reasonable)?

[para 29] Section 11(1) of PIPA limits the purposes for which personal information may be collected to those that are reasonable. It states:

> *11(1) An organization may collect personal information only for purposes that are reasonable.*

[para 30] Section 16(1) states:

> *16(1) An organization may use personal information only for purposes that are reasonable.*

[para 31] Section 19(1) states:

> *19(1) An organization may disclose personal information only for purposes that are reasonable.*

[para 32] I found, above, that the evidence establishes that the Organization collected the Complainant's personal information for the purpose of participating in legal proceedings. As section 14(1)(d) expressly authorizes organizations to collect, use, and disclose personal information without consent for the purpose of legal proceedings, I accept that the Legislature determined that collection for the purpose of legal proceedings is a reasonable purpose. There is no evidence before me to establish that the organization collected personal information for any other purpose than participating in legal proceedings.

[para 33] The Complainant has not adduced evidence that raises the possibility that the Organization collected and used the Complainant's personal information in the circumstances he alleges, or for any unreasonable purposes. I conclude that the Complainant has not met the evidential burden with regard to sections 11(1), (16)(1) and 19(1).

ISSUE D: Did the Organization collect, use or disclose the information contrary to, or in accordance with, sections 11(2), 16(2) and 19(2) of PIPA (collection, use and/or disclosure to the extent reasonable for meeting the purposes)?

[para 34] Section 11(2) states:

> *11(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected*

[para 35] Section 16(2) states:

> *Where an organization uses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is used.*

[para 36] Section 19(2) states:

> *19(2) Where an organization discloses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is disclosed.*

[para 37] The Complainant argues:

> It is also not reasonable for Hi Line to collect all of the personal information held on [the Complainant's] phone, when that information is not relevant whatsoever to the legal proceedings. The scope of collection and use of [the Complainant's] personal information is far too broad to be reasonably justified by an investigation into legal proceedings. Obviously the bulk of [complainant's] personal information is irrelevant to that purpose. It is also not reasonable for Hi Line to collect all of the personal information held on [the] phone, when that information is not relevant whatsoever to the legal proceedings. The scope of collection and use of [the Complainant's] personal information is far too broad to be reasonably justified by an investigation into legal proceedings. Obviously the bulk of [the Complainant's] personal information is irrelevant to that purpose.

[para 38] As noted above, I have found the majority of information that is the subject of the complaint is not the Complainant's personal information, as it is not about him. However, I found that some information, such as statements about the Complainant's health, his views about a family funeral and a family member are his personal information.

[para 39] The Organization accessed its own Apple iCloud account and produced the information it located for the litigation in which it is involved, including the information I have found to be personal information. I understand that the Complainant does not consider it relevant to the proceedings. However, section 11(2) does not require personal information to be relevant, only that an organization not collect more personal information than was necessary for meeting its purpose of preparing for litigation. It has not been demonstrated that the Organization collected more information than was necessary for meeting its purpose, given that it all the information that is the subject of the complaint was produced by it in litigation. In other words, it appears that all the information it collected was then used by the Organization for the litigation.

[para 40] As discussed above, much of the information that is the subject of the complaint is not personal information. Moreover, it is not a collection for an organization to review information in its files or on its systems to determine what belongs to it, or what is personal information or not. It is a collection once the Organization gathers it for a purpose, in this case, use in litigation. The Organization appears to have collected only the personal information it had decided was necessary for the litigation in which it was involved and used it for that same purpose. As noted above, the Complainant has not

adduced any information to suggest that the Organization collected, used, and disclosed his personal information in the circumstances alleged, that is, without authority, or for an unauthorized purpose.

IV. ORDER

[para 41] I make this Order under section 52 of the Act.

[para 42] I find that it has not been established that the Organization collected, used, or disclosed the Complainant's personal information without authority or for an unauthorized purpose. I also find that there is no evidence to support finding that the Organization collected, used, or disclosed the Complainant's personal information in contravention of PIPA.

_____

Teresa Cunningham
Adjudicator
/bah