In the Court of Appeal of Alberta

Citation: Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner), 2011 ABCA 94

Date: 20110328
Docket: 0901-0223-AC
Registry: Calgary

Between:

Leon's Furniture Limited

Appellant
(Applicant)

- and -

The Information and Privacy Commissioner of Alberta

Respondent
(Respondent)

- and -

Sharon Curtis

Not a Party to the Appeal
(Respondent)

- and -

The Attorney General of Alberta

Not a Party to the Appeal
(Respondent)

The Court:

The Honourable Madam Justice Carole Conrad
The Honourable Mr. Justice Ronald Berger
The Honourable Mr. Justice Frans Slatter

Reasons for Judgment Reserved of the Honourable Mr. Justice Slatter
Concurred in by the Honourable Mr. Justice Berger

Dissenting Reasons for Judgment Reserved of the Honourable Madam Justice Conrad

Appeal from the Judgment by
The Honourable Madam Justice R. Nation
Dated the 18th day of June, 2009
Filed on the 25th day of June, 2009
(Docket: 0801-12471)

Reasons for Judgment Reserved
of the Honourable Mr. Justice Slatter

[1] The issue on this appeal is whether it was reasonable for the Privacy Commissioner to prohibit the appellant from collecting driver's licence numbers from customers when they or someone on their behalf pick up furniture.

Facts

[2] The appellant is a furniture retailer. In 2006 a customer purchased a table from the appellant, and paid a deposit, but did not take immediate delivery. The customer told the appellant's staff that her mother would be coming to pick up the table.

[3] The next month the customer's mother arrived to pick up the table. She paid the balance owing, and was required to produce her driver's licence before she could take delivery of the table. Despite her objection, the sales clerk recorded the driver's licence number on the "pick ticket". The pick ticket does not have the customer's name recorded on it, but it can obviously be correlated back to the original sales invoice which contains the customer's name and address. The appellant had measures in place to protect the information, which was not stored on a computer system.

[4] The customer's mother then proceeded to the loading dock. The staff member at the loading dock asked the customer's mother to sign on a separate pick ticket an acknowledgment that she had picked up the table, and also to record the vehicle licence plate number of her car. The customer's mother objected, but complied. The customer's mother subsequently filed a complaint with the respondent Commissioner about the collection of her driver's licence and vehicle licence numbers.

The Delegate's Decision

[5] The respondent Commissioner initiated an investigation, and delegated the matter to a staff member to conduct an inquiry.

[6] The appellant acknowledged its policy of collecting driver's licence and licence plate numbers in order to deter, prevent, and detect fraud. Particular risks arise when the furniture is not delivered on purchase. The furniture may be picked up later by family members, friends, interior designers, contractors, or delivery companies. Sometimes furniture is purchased in one city and picked up in another.

[7] Two potential categories of fraud were identified:

- Situations where a stranger fraudulently picks up the furniture without the authority of the customer. This would be a particularly acute problem when a third party is authorized to pick up the furniture.

- Situations when the customer picks up the furniture, but later denies getting the furniture that was paid for, or refuses to pay in the future based on an allegation that the furniture was never received.

The appellant argued that its policy protects itself and the customer, and was also of assistance to the police when it became necessary to investigate fraud. The appellant noted that it stored the numbers separately from the names and addresses of the customers, thereby limiting the potential for misuse of the information. There is nothing on the record to support the complainant's concern that the personal information collected was shared with third parties, or used for marketing or other collateral purposes.

[8] The adjudicator rejected the appellant's contention that driver's licence and licence plate numbers are not "personal information" as that term is defined in the *Personal Information Protection Act*, R.S.A. 2000, c. P-6.5: ***Leon's Furniture Ltd.***, Order P2008-004, August 27, 2008.

[9] The adjudicator commenced the analysis by deciding that the collection of the disputed information was not "reasonable", under s. 11. The adjudicator appeared to treat reasonableness as a freestanding basis for collecting the information, regardless of whether the complainant had consented. When the Court requested further submissions on the point, both parties agreed that s. 11 imposes a requirement of "reasonableness" in addition to the need for consent, and "reasonableness" would not itself justify collection of the information. Nevertheless, the reasonableness of the collection of the information is a consideration that arises under other applicable sections, such as s. 7(2).

[10] The adjudicator accepted that preventing fraud and theft is a reasonable purpose for collecting personal information. She concluded, however, that recording the driver's licence and licence plate numbers went beyond what was necessary for preventing fraudulent pickup. The adjudicator concluded that it was reasonable only to record the name and address of the person picking up the furniture, and to examine the identification produced to verify the identity of the person, but that it was not reasonable to record the number of the identification being used. She did not explain why it was reasonable to record the person's name and address, when that too is "personal information".

[11] The adjudicator also went on to conclude that the appellant was in violation of s. 7(2) of the *Act*, which prevents making it a condition of "supplying a product or service" that the customer provide personal information beyond what is necessary to supply the product or service. The

adjudicator considered that picking up furniture after the time of sale is a "service" that the appellant would not provide unless identification was produced.

[12] The adjudicator concluded that the appellant was also in violation of s. 13 of the *Act* because it did not explain to the complainant the reason for the collection of the personal information, except that it was "store policy".

[13] As a remedy, the adjudicator ordered that the appellant cease recording driver's licence and licence plate numbers when an individual is picking up merchandise. She also directed that the appellant destroy all existing records of driver's licence and licence plate numbers. The inquiry did not examine, and no remedy was given with respect to the appellant's practices for the safe and secure storage of the numbers, nor with respect to the length of time that the numbers are retained on file.

Judicial Review

[14] The appellant's application for judicial review of the respondent's decision was dismissed. The chambers judge concluded that the standard of review is reasonableness, and that the decision of the adjudicator was reasonable. The chambers judge did not agree that the adjudicator had unreasonably focussed on the purpose of the policy being the prevention of fraud, as opposed to the detection of fraud after it occurs. The chambers judge concluded that there was considerable overlap between the protection of the appellant and its customers, deterring fraud, and detecting the responsible party once fraud occurs. The chambers judge did not agree that the adjudicator failed to balance the interests of the appellant and its customers, as required by the *Act*.

Issues on Appeal

[15] The following issues arise for discussion and decision:

- the standing of the respondent Commissioner to make submissions in this appeal;
- the standard of review of the respondent's decision;
- the scheme of the *Act* and the overall approach of the adjudicator;
- whether driver's licence and licence plate numbers are "personal information";
- whether the appellant's provision of services conditional on the provision of personal information was reasonably necessary;
- whether the appellant adequately communicated its policy to its customers.

<u>Standing of the Commissioner</u>

[16] The appellant challenges the standing of the respondent Commissioner to make submissions on the merits of the appeal. The appellant relies on a long series of cases which hold that an administrative tribunal is free to argue issues of jurisdiction or to explain the record when its decisions are subject to judicial review, but it should not enter the arena and argue the correctness of its decision. That line of cases starts with ***Northwestern Utilities v. Edmonton (City)***, [1979] 1 S.C.R. 684, and the issue was recently discussed in ***Brewer v. Fraser Milner Casgrain LLP***, 2008 ABCA 160, 90 Alta. L.R. (4th) 201, 432 A.R. 188.

[17] ***Northwestern Utilities*** arose from a rate setting decision of the Public Utilities Board. The City of Edmonton appealed the decision to the Appellate Division of the Supreme Court of Alberta, which set aside the decision and remitted the matter back to the Board for reconsideration. Both Northwestern Utilities and the Board appealed that decision to the Supreme Court of Canada. The City of Edmonton actively participated in response. In addition to dealing with the substantive issues on the appeal, the Court commented on the participation of the Board in the proceedings.

[18] The Court in ***Northwestern Utilities*** concluded that while the statute gave the Board a right to appeal and a right of audience on the appeal, its proper role was limited. The statute drew a distinction between the full "parties" to the appeal, and the Board itself. The Court noted at p. 709 that vigorous arguments in support of the Board's own decision effectively amounted to arguments in support of one of the adverse parties. The Board had its opportunity to state its reasons in its decision, and "it abuses one's notion of propriety to countenance its participation as a full-fledged litigant in this Court, in complete adversarial confrontation with one of the principals in the contest before the Board itself". The party against whom the Board was presently arguing might well have to appear before the Board in the future, perhaps on the same or a similar issue, creating the potential for an apprehension of bias. As a result it was "the policy in this Court to limit the role of an administrative tribunal whose decision is at issue before the Court . . . to an explanatory role with reference to the record before the Board and to the making of representations relating to jurisdiction" (at p. 709). Particular restraint was required when the proceedings of the tribunal were attacked as being contrary to the rules of natural justice, because in those cases the tribunal's own conduct was under examination.

[19] The ***Brewer*** decision involved a different point: whether the Human Rights Commission had a right to launch an appeal, an issue on which the Commission clearly had standing. In concluding that there was no right of appeal, the Court analogized from the ***Northwestern Utilities*** principle, reasoning that since the role of the tribunal was at best limited, the language of the statute should not be stretched to provide a right of appeal in the first place. The *obiter dictum* in ***Brewer*** stated the ***Northwestern Utilities*** principle in absolute terms. The *obiter dictum* statements appear to be

inconsistent with an earlier uncited decision of this Court: ***Rockyview (Municipal District No. 44) v. Alberta (Planning Board)*** (1982), 22 Alta. L.R. (2d) 87, 40 A.R. 344 (C.A.).

[20] The ***Northwestern Utilities*** principle is easiest to apply in situations where the tribunal is exercising what would at the time of that decision have been called "judicial or quasi-judicial functions". Where an applicant and a respondent are present and are participating fully in the proceedings before the tribunal, and then before the court on judicial review (as was the case in ***Northwestern Utilities***), there is little need for the tribunal to be involved. Where the tribunal is adjudicating over a dispute between two adversarial parties, it is especially important that the tribunal remain neutral.

[21] But not all administrative tribunals perform adjudicative functions. Many of them receive and investigate complaints, and can generate complaints themselves. They often have an important policy making role, as well as an educational role within their sphere of activity. Often their adjudicative and policy making roles cannot be separated. If their investigations reveal a breach of the regulatory regime, some tribunals essentially take over the prosecution of the complaint, and effectively have carriage of the entire proceeding. They become the investigator, prosecutor, and adjudicator. The original complainant does not and is not expected to participate, except possibly as a witness. In some cases the complainant cannot even settle the complaint without the consent of the tribunal: *Canadian Human Rights Act*, R.S.C. 1985, c. H-6, s. 48. In these situations the applicability of the ***Northwestern Utilities*** principle is less obvious.

[22] Further, it is clear that what was considered at the time of ***Northwestern Utilities*** to be a "jurisdictional" issue (on which submissions by the tribunal were acceptable) was a much wider concept than it is after ***Dunsmuir v. New Brunswick***, 2008 SCC 9, [2008] 1 S.C.R. 190.

[23] On many judicial review applications it is quite obvious to the chambers judge that if the tribunal does not make submissions in support of the decision under review, no submissions will be made. The applicant's arguments and authorities on the merits will essentially be unanswered. Some tribunals will justify their appearances on the basis that otherwise "no one shows up": ***Skyline Roofing Ltd. v. Alberta (Workers' Compensation Board)***, 2001 ABQB 624, 95 Alta. L.R. (3d) 126, 292 A.R. 86 at para. 29. The adversarial system requires the presentation and consideration of competing arguments and ideas on the reasonableness or correctness of the decision under review. Rather than essentially proceeding to decide the application *ex parte*, many judicial review judges will receive submissions from the tribunal for "forensic" reasons: ***Beier v. Vermilion River (County)***, 2009 ABCA 151, 457 A.R. 191 at para. 8.

[24] The case law recognizes that some flexibility is required when defining the proper role of tribunals in judicial review proceedings. In ***CAIMAW v. Paccar of Canada Ltd.***, [1989] 2 S.C.R. 983 at p. 1016 the Supreme Court of Canada quoted with approval the following passage from ***B.C.G.E.U. v. Industrial Relations Council*** (1988), 26 B.C.L.R. (2d) 145 (C.A.):

> The traditional basis for holding that a tribunal should not appear to defend the correctness of its decision has been the feeling that it is unseemly and inappropriate for it to put itself in that position. But when the issue becomes, as it does in relation to the patently unreasonable test, whether the decision was reasonable, there is a powerful policy reason in favour of permitting the tribunal to make submissions. That is, the tribunal is in the best position to draw the attention of the court to those considerations, rooted in the specialized jurisdiction or expertise of the tribunal, which may render reasonable what would otherwise appear unreasonable to someone not versed in the intricacies of the specialized area. In some cases, the parties to the dispute may not adequately place those considerations before the court, either because the parties do not perceive them or do not regard it as being in their interest to stress them.

The Court in ***Paccar*** went on to hold at p. 1017:

> The argument before us emphasized that the Council had made a careful review of the relevant authorities and had made a decision that was within its exclusive jurisdiction. At no point did it argue that the decision of the Board was correct. Rather it argued that it was a reasonable approach for the Board to adopt. The Council had standing to make all these arguments, and in doing so it did not exceed the limited role the Court allows an administrative tribunal in judicial review proceedings.

Three members of the Court in ***Paccar*** agreed with this approach, and the other three did not comment on the issue.

[25] It has been argued that a rigid application of the ***Northwestern Utilities*** principle is inconsistent with the functional and pragmatic approach now used in administrative law. As argued by L. A. Jacobs and T.S. Kuttner, *Discovering What Tribunals Do: Tribunal Standing Before the Courts* (2002), 81 Can. Bar Rev. 616 at p. 645:

> We suggest that the cases be approached within the context of the general shift in the jurisprudence from formalism to functionalism, as epitomized in the pragmatic and functional approach now characteristic of administrative law decisions across a broad band of issues. Within the particular sphere that we are addressing here - the discourse between courts and tribunals in the arena of judicial review - it is not immediately apparent that the courts have embraced the functional over the formal.

Similar arguments have been made in N. Semple, "*The Case for Tribunal Standing in Canada*" (2007), 20 C.J.A.L.P. 305 and F. Falzon, "*Tribunal Standing on Judicial Review*" (2008), 21 C.J.A.L.P. 21. This approach has now been adopted in some cases.

[26] In ***Ontario (Children's Lawyer) v. Ontario (Information and Privacy Commissioner***) (2005), 75 O.R. (3d) 309 (C.A.) the Court accepted the argument of the parties that the permissible role of a tribunal in a particular proceeding is in the discretion of the court, and depends on the particular context. Rigid rules should be avoided. The Court agreed on the importance of maintaining the impartiality of the tribunal, but also noted the importance of having all the relevant information and arguments put forward. Goudge J.A., speaking for a unanimous Court, put it this way:

> [34] However, I agree with the parties that a context-specific solution to the scope of tribunal standing is preferable to precise *a priori* rules that depend either on the grounds being pursued in the application or on the applicable standard of review. For example, a categorical rule denying standing if the attack asserts a denial of natural justice could deprive the court of vital submissions if the attack is based on alleged deficiencies in the structure or operation of the tribunal, since these are submissions that the tribunal is uniquely placed to make. Similarly, a rule that would permit a tribunal standing to defend its decision against the standard of reasonableness but not against one of correctness, would allow unnecessary and prevent useful argument. Because the best argument that a decision is reasonable may be that it is correct, a rule based on this distinction seems tenuously founded at best as Robertson J.A. said in *United Brotherhood of Carpenters and Joiners of America, Local 1386 v. Bransen Construction Ltd.*, [2002] N.B.J. No. 114, 249 N.B.R. (2d) 93 (C.A.), at para. 32.
>
> [35] Nor do I think cases like *Northwestern* and *Paccar*, *supra*, dictate the use of precise rules of this sort. Particularly in light of the recent evolution of administrative law away from formalism and towards the more flexible practical approach exemplified by *Pushpanathan v. Canada (Minister of Citizenship and Immigration)*, [1998] 1 S.C.R. 982, [1998] S.C.J. No. 46, I think these cases are best viewed as sources of the fundamental considerations that should inform the court's discretion in the context of a particular case. Resolving the scope of standing on this basis rather than by means of a set of fixed rules is likely to produce the most effective interplay between the array of different administrative decision-makers and the courts.

In the result, in that case the Privacy Commissioner was allowed to fully participate in the judicial review application. The Court, however, noted at para. 61 that the tribunal should "pay careful attention to the tone with which it does so . . . A tribunal that seeks to resist a judicial review application will be of assistance to the court to the degree its submissions are characterized by the helpful elucidation of the issues, informed by its specialized position, rather than by the aggressive partisanship of an adversary."

[27] This Court previously adopted this approach in ***Rockyview (Municipal District No. 44)***. A more flexible approach has also been suggested in other provinces: ***United Brotherhood of Carpenters and Joiners of America, Local 1386 v. Bransen Construction Ltd.***, 2002 NBCA 27, 249 N.B.R. (2d) 93 at para. 32; ***Global Securities Corp. v. British Columbia (Executive Director, Securities Commission***), 2006 BCCA 404, 56 B.C.L.R. (4th) 79 at para. 60.

[28] I agree that the law should acknowledge the multifaceted roles of many modern administrative tribunals, and the realities of the situation. The ***Northwestern Utilities*** case should be used as a "source of the fundamental considerations". Its principle will often be applied with full vigour to administrative tribunals that are exercising adjudicative functions, where two adverse parties are present and participating. While the involvement of a tribunal should always be measured, there should be no absolute prohibition on them providing submissions to the court. Whether the tribunal will be allowed to participate, and the extent to which it should participate involves the balancing of a number of considerations.

[29] It is not possible to compile a list of all the relevant factors to consider when the appropriate level of participation of a tribunal is being established. The existence of other parties who can effectively make the necessary arguments is a central consideration. For example, in ***Skyline Roofing*** the challenge was to a decision of the Workers' Compensation Appeals Commission, and the Workers' Compensation Board (not the Commission) was the appropriate party to make the arguments. Maintaining the appearance of independence and impartiality of the tribunal is also a key consideration. The effect of tribunal participation on the overall fairness (in fact and in appearance) of the proceedings is a relevant consideration. Of importance too is the role assigned to the tribunal under the statute. Where the statute effectively gives carriage of the proceedings to the tribunal, a greater level of participation is tolerable: ***British Columbia Teachers' Federation v. British Columbia (Information and Privacy Commissioner***), 2005 BCSC 1562, 50 B.C.L.R. (4th) 151 at para. 45. The nature of the proposed arguments is important. A tribunal should not be allowed to supplement its reasons for decision, or to attempt to provide fresh justifications for the result: ***Bransen Construction*** at para. 33. While the tribunal, like any other party, can offer interpretations of its reasons or conclusion, it cannot attempt to reconfigure those reasons, add arguments not previously given, or make submissions about matters of fact not already engaged by the record. A tribunal can, within those limits, attempt to rebut arguments about how it reasoned and what it decided.

[30] The *Personal Information Protection Act* gives the Commissioner a wide ranging responsibility to implement the *Act*, to develop privacy policy, to educate, and to investigate and adjudicate upon complaints. After a complaint is made, carriage of the complaint effectively passes to the Commissioner. If the Commissioner concludes that the complaint warrants further

proceedings, the Commissioner's staff prosecutes the complaint, and a delegate appointed by the Commissioner will rule on it. For better or for worse, the Commissioner wears many hats, and he is not merely an adjudicator detached from the dispute itself. The Commissioner is very close to being a true party. It is unrealistic to think that the original complainant would have the resources or the motivation to resist the application for judicial review. If the Commissioner does not resist the judicial review application, no one will. In the circumstances, the Commissioner should be afforded some latitude in the submissions that he can make to the court. In this appeal neither the content of the respondent's arguments, nor their tone, exceed what is appropriate, and the Commissioner's participation, on this record, is unobjectionable.

Standard of Review

[31] In ***Macdonell v. Quebec (Commission d'accès à l'information)***, 2002 SCC 71, [2002] 3 S.C.R. 661 at para. 8 the Court held:

> The Quebec Commission d'accès à l'information has no special interest in the decision it must make, and so it is able to play its role independently. By virtue of the fact that it is always interpreting the same Act, and that it does so on a regular basis, the Quebec Commissioner develops general expertise in the field of access to information. That general expertise on the part of the Commission invites this Court to demonstrate a degree of deference.

In ***Macdonell***, the Court found it appropriate to apply a standard of reasonableness to the decision of the Commissioner. It is perhaps questionable whether any single issue tribunal truly has "no interest in its decisions", as all such tribunals have a philosophy about their work: ***Bransen Construction*** at para. 16. But so long as that philosophy is consistent with a reasonable interpretation of the statute, that is unobjectionable.

[32] In this appeal both parties submitted that the proper standard of review of the adjudicator's decision is "reasonableness". Interpreting the definition of "personal information" is a question of law, but it is one within the core function of the adjudicator. Determining whether the practices of the appellant are "reasonable" is a mixed question of fact, law and policy. While there is not a strong privative clause in the statute, the nature of these questions, given the role of the Commissioner and the adjudicators appointed by him, calls for review on the reasonableness standard: ***Stubicar v. Alberta (Office of the Information and Privacy Commissioner)***, 2008 ABCA 357, 97 Alta. L.R. (4th) 23, 440 A.R. 190 at paras. 22-4.

[33] As will be seen (*infra*, para. 38), s. 2 of the statute contains a definition of "reasonable", which is what "a reasonable person would consider appropriate in the circumstances". Section 2 defines "reasonable" as a pure objective standard. It is not the ***Dunsmuir*** test. The standard of review is also reasonableness, but in the ***Dunsmuir*** sense. So one issue is whether it was

"***Dunsmuir***" unreasonable for the adjudicator to find that it was "objectively" unreasonable for the appellant to keep the personal information. The test in ***Dunsmuir*** is as follows:

> 47 Reasonableness is a deferential standard animated by the principle that underlies the development of the two previous standards of reasonableness: certain questions that come before administrative tribunals do not lend themselves to one specific, particular result. Instead, they may give rise to a number of possible, reasonable conclusions. Tribunals have a margin of appreciation within the range of acceptable and rational solutions. A court conducting a review for reasonableness inquires into the qualities that make a decision reasonable, referring both to the process of articulating the reasons and to outcomes. In judicial review, reasonableness is concerned mostly with the existence of justification, transparency and intelligibility within the decision-making process. But it is also concerned with whether the decision falls within a range of possible, acceptable outcomes which are defensible in respect of the facts and law.

The Scheme of the *Act*

The Overall Purpose

[34] The *Personal Information Protection Act* expressly states its overall purposes. This is a key to any interpretation and application of the statute. The most important provision is s. 3:

> 3 The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable. (Emphasis added)

The statute recognizes two competing values: the right to protect information, and the need to use it. When Bill 44 was discussed in Committee, the Minister of Government Services stated:

> When it comes to the reasonable standards in section 2, the bill sets the standard for compliance with the act, and that standard is the reasonableness standard. This standard is important because it ensures that the act is flexible for small and medium-sized businesses. If businesses act reasonably, they have no problem with complying with the act. (*Hansard*, November 25, 2003)

The statute does not give predominance to either of the two competing values, and any interpretation which holds that one must always prevail over the other is likely to be unreasonable. A balancing is called for. That balancing is not fully implemented by the other provisions of the *Act*. The balance called for by s. 3 must also be maintained by the Commissioner when assessing what is “reasonable”.

[35] The issue is not whether privacy rights are important. They are, as demonstrated by the cases discussed by Conrad J.A. at paras. 102-114.The Legislature has deemed them to be important by passing the *Act*. But their admitted importance does not mean that privacy rights must predominate over all other societal needs, values and interests. Because the customer’s interests are important does not mean the retailer’s are not. Our society is complex and increasingly information based, and many organizations, businesses and individuals must use personal information for legitimate reasons on a daily basis. An unreasonable curtailment of the ability to use that information imposes a financial and social burden which is recognized by s. 3 of the *Act*. The *Act* recognizes that a balancing of the various interests is called for, and it is inconsistent with any suggestion that privacy rights should always predominate over competing values. The statute cannot reasonably be interpreted in a way that prevents reasonable uses of personal information.

[36] The *Act* makes frequent use of the concepts of “reasonableness” and “consent”.

Reasonableness

[37] A number of provisions in the statute require that information be used, or the right to use information be exercised, in a “reasonable” manner. There is an overriding provision in s. 5(5) that: “In meeting its responsibilities under this Act, an organization must act in a reasonable manner.” Section 11(1) confirms that: “An organization may collect personal information only for purposes that are reasonable.” Sections 16 and 19 apply the same test to the use and disclosure of information.

[38] The statute provides a definition of “reasonable”:

> 2 Where in this Act anything or any matter
>
> (a) is described, characterized or referred to as reasonable or unreasonable, or
>
> (b) is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner,
>
> the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances.

This section essentially embraces the common law concept of the "reasonable person", and provides that the conduct of organizations using personal information must be scrutinized accordingly. The hypothetical reasonable person would recognize both of the values set out in s. 3: the rights of individuals to a reasonable level of privacy, and the needs of organizations to make reasonable use of information in the conduct of their activities.

[39] The approach of the adjudicator and the position of the respondent are in several respects not in accord with these provisions of the statute, and are in that respect unreasonable. Some examples include:

- "An important element of the balancing to be conducted under s. 11 is the recognition that an individual's right to privacy is paramount to an organization's need to collect information." (Respondent's factum, para. 93). This is not an interpretation of s. 3 and 11 that is reasonably open; it is not reasonably possible to interpret s. 3 as saying one of the values in s. 3 is paramount over the other.

- "By and large, the federal and provincial Privacy Commissioners have agreed with those Canadians who think that recording driver's licence numbers is excessive. The Commissioners understand the organizations' reasons, but they tend to think that they go too far by recording the numbers." "The same goal of due diligence may be accomplished in other less privacy-invasive ways." "Rule of thumb: Retailers should collect the least amount of personal information possible to satisfy legitimate business activity." (*Collection of Driver's Licence Numbers under Private Sector Privacy Legislation: a Guide for Retailers*, policy statement of the Privacy Commissioner of Alberta and others). The statute does not require the organization to prove it has adopted a "minimalist" approach to the collection of data, only that it has acted reasonably. These statements are not a reasonable interpretation of the *Act*.

- ". . . ensuring that the person picking up the item is either the customer that purchased the item or someone authorized by the customer to pick it up is the best way to prevent fraud in these instances." (Adjudicator's reasons, para. 24). The statute does not require the organization to prove that it has adopted what the respondent finds to be the "best" way, only that the way it has chosen is reasonable.

- "[Recording driver's licence numbers] goes beyond what is necessary for the purpose of preventing fraudulent pick ups, or confirming the identity of the person picking up merchandise." ". . . organizations should ensure that they are not collecting identity information unless it is <u>necessary</u> for the transaction." (Adjudicator's reasons, paras. 27, 32). The appellant does not always have to prove necessity, only reasonableness.

While the reviewing court should extend deference to the respondent's interpretation of the statute, the respondent cannot adopt interpretations of the statute that it cannot reasonably bear. An interpretation that is not harmonious with the context and the overall scheme of the statute is unlikely to be one reasonably available on the facts and the law: ***IMS Health Canada, Ltd. v. Alberta (Information and Privacy Commissioner)***, 2008 ABQB 213, 93 Alta. L.R. (4th) 12, 442 A.R. 268 at paras. 101-2. It is not open to the respondent to change "reasonableness" to either "necessity", "minimal intrusion", or "best practices". These are not interpretations that are available given the plain wording of the statute.

[40] Many Albertans rely on their driver's licences on a daily basis to prove who they are for various legitimate reasons, such as making purchases on credit or boarding airplanes. Driver's licences are not just proof that the holder is authorized to drive; the average Albertan uses his or her driver's licence far more frequently to prove identity than to prove the right to drive. The Federal, Alberta, and British Columbia Privacy Commissioners have jointly produced a document entitled *Collection of Driver's Licence Numbers Under Private Sector Privacy Legislation – A Guide for Retailers*, which states in part:

> A driver's licence is not a universal identity card. Rather, it is a means to enforce traffic laws and offer proof that someone is authorized to operate a motor vehicle. The driver's licence number is sensitive and valuable to those intent on committing identity crimes. For this reason, these numbers are often the subject of security attacks and misuse.

This reasoning is internally inconsistent. If a driver's licence is "not a universal identity card", then why is it of any interest to "those intent on committing identity crimes"? As the Commissioners note in their *Guide for Retailers*, the driver's licence is a government issued, reliable, and generally acceptable method of proving identity. That is the source both of its value and its potential for abuse.

[41] In determining what use of driver's licence numbers would be found to be "appropriate in the circumstances" by "reasonable persons", one must therefore have regard to the important place that driver's licences play as a universal form of identification:

> Driver's licences . . . have become a near universal form of identification. The integrity and reliability of the driver's licence system benefits all Albertans who require, on a routine basis, proof of their identity. ***Hutterian Brethren of Wilson Colony v. Alberta***, 2007 ABCA 160, 417 A.R. 68, 77 Alta. L.R. (4th) 281 at para. 127, quoted with approval on appeal *sub nom.* ***Alberta v. Hutterian Brethren of Wilson Colony***, 2009 SCC 37, [2009] 2 S.C.R. 567 at paras. 41, 140.

The driver's licence is such an important form of identification that the government has established a parallel system of identification cards for persons who, for whatever reason, do not qualify for a driver's licence: *Identification Card Regulation*, Alta. Reg. 221/2003, pursuant to the *Government Organization Act*, R.S.A. 2000, c. G-10; ***Hutterian Brethren v. Alberta***, 2007 ABCA 160 at para. 64. While protecting Albertans from invasions of privacy, intrusive marketing practices, and identity theft are laudable objectives, it is unreasonable to place restrictions on the use of driver's licences that seriously undermine their usefulness as forms of identification. Section 3 of the *Act* specifically recognizes that individuals and organizations all have legitimate reasons to use personal information in this way.

Consent

[42] Along with "reasonableness", "consent" is a principle that permeates the *Act*. Section 7(1) provides that "except where this Act otherwise provides", information about an individual must not be collected without the individual's consent. Sections 12 and 14 contain some specific exceptions to this principle, and expressly allow some collection of information "without consent". Both parties to this appeal agreed that s. 11, which requires that the collection of personal information be reasonable, is a condition in addition to the general requirement of consent, and is not an exception to the need for consent.

[43] "Consent" under the *Act* is a nuanced concept. Consent may obviously be overtly and willingly given. However, s. 8(2) provides for situations where an individual is "deemed to consent". This section may, to summarize, be described as recognizing acquiescence in the collection of personal information. Section 8(3) permits the collection of information without consent where notice is given of the intention to collect information, and no timely objection is made. Section 14(a) allows the collection of information without consent where it seems reasonable to think that collecting the information is in the best interests of the individual. (The rest of s. 14 lists a number of instances where for policy reasons consent is not required.)

[44] Of importance to this appeal is s. 7(2) of the *Act* which reads:

> (2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

This provision imposes a prohibition on unnecessary contractual terms requiring the disclosure of personal information, but it does provide for what might be called "reluctant consent". The individual does not really want to provide the personal information, but does want to take advantage of the products or services that are available if the information is provided. The *Act* allows an organization to refuse to contract except on the basis that personal information will be provided, so long as that condition of the contract is reasonably necessary (see *infra*, para. 54).

[45] In this case it is clear that the complainant did not willingly consent to providing her personal information. She emphatically objected. The appellant argued that even though she objected, in the end she did provide the requested personal information in order to get possession of the table, and therefore she did actually consent. That form of "reluctant consent" must be justified under s. 7(2) of the *Act* if it is to be recognized. Other customers who without objection provided the same sort of information in similar circumstances may well have acquiesced within the meaning of s. 8(2). The order of the adjudicator that all the information collected from every customer be destroyed was therefore overbroad, as the appellant was entitled to record information provided through acquiescence, so long as it was reasonably necessary for the appellant's business. But the particular complainant in this case did not fall into the acquiescence category.

<u>What Is "Personal Information"?</u>

[46] The adjudicator rejected the appellant's argument that driver's licence numbers and vehicle licence numbers do not fall within the definition of "personal information" in the statute:

> 1(1) In this Act,
>
> . . .
>
> (k) "personal information" means information about an identifiable individual.

The appellant argues that neither a driver's licence number, nor a licence plate number, fall within this definition.

[47] The "identifiable individual" term has two components. Firstly, the individual must be "identifiable". Generic and statistical information is thereby excluded, and the personal information (here the relevant number) must have some precise connection to one individual. Secondly, the information must relate to an individual. Information that relates to objects or property is, on the face of the definition, not included. The key to the definition is the word "identifiable". The *Act* is designed to regulate and protect information that is uniquely connected to one person. An important (although not the only) purpose of the *Act* is to control the use of information that would enable "identity theft", that is, information that is used to distinguish one individual from another in financial and commercial transactions. This can be seen by reviewing the type of information that is dealt within the more specific provisions and exceptions in the *Act*. The definition is not primarily aimed at information about that individual's opinions, choices and status in life.

[48] Further, to be "personal" in any reasonable sense the information must be directly related to the individual; the definition does not cover indirect or collateral information. Information that relates to an object or property does not become information "about" an individual, just because some individual may own or use that property. Since virtually every object or property is connected in some way with an individual, that approach would make all identifiers "personal" identifiers. In the context of the statute, and given the purposes of the statute set out in s. 3, it is not reasonable to expand the meaning of "about an individual" to include references to objects that might indirectly be affiliated or associated with individuals. Some identification numbers on objects may effectively identify individuals. Many, however, are not "about the individual" who owns or uses the object, they are "about the object".

[49] The adjudicator's conclusion that the driver's licence number is "personal information" is reasonable, because it (like a social insurance number or a passport number) is uniquely related to an individual. With access to the proper database, the unique driver's licence number can be used to identify a particular person: ***Gordon v. Canada (Minister of Health)***, 2008 FC 258, 324 F.T.R. 94, 79 Admin. L.R. (4th) 258 at paras. 32-4. But a vehicle licence is a different thing. It is linked to a vehicle, not a person. The fact that the vehicle is owned by somebody does not make the licence plate number information about that individual. It is "about" the vehicle. The same reasoning would apply to vehicle information (serial or VIN) numbers of vehicles. Likewise a street address identifies a property, not a person, even though someone may well live in the property. The licence plate number may well be connected to a database that contains other personal information, but that is not determinative. The appellant had no access to that database, and did not insist that the customer provide access to it.

[50] It is also contrary to common sense to hold that a vehicle licence number is in any respect private. All vehicles operated on highways in Alberta must be registered, and must display their licence plates in a visible location: *Traffic Safety Act*, R.S.A. 2000, c. T-6, ss. 52(1)(a) and 53(1)(a). The requirement that a licence plate be displayed is obviously so that anyone who is interested in the operation of that vehicle can record the licence plate. The fact that the licence plate number might be connected back to personal information about the registered owner is obvious, but the *Traffic Safety Act* nevertheless requires display of the licence plate. Control of that information is provided by controlling access to the database. It makes no sense to effectively order, as did the adjudicator, that everyone in the world can write down the customer's licence plate number, except the appellant.

[51] In summary, the adjudicator's conclusion that a driver's licence number is "personal information" is reasonable. The conclusion that a licence plate number is also "personal information" is not reasonable, and the adjudicator's ruling must be set aside insofar as it dealt with licence plate numbers.

Providing Goods on Condition

[52] As previously noted, the complainant did not willingly provide her personal information. She was faced with a dilemma: she either had to give her personal information, or she had to leave without her daughter's table. By virtue of the policies it had in place, the appellant essentially was not prepared to contract except on the basis that if a third party picked up the furniture, certain personal information would be required. This engaged section 7(2) of the *Act*:

> 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,
>
> (c) use that information unless the individual consents to the use of that information, or
>
> (d) disclose that information unless the individual consents to the disclosure of that information.
>
> (2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

The adjudicator concluded that the appellant was in breach of s. 7(2).

[53] Section 7(2) is primarily ancillary to s. 7(1). The provisions of s. 7(2) are designed to prevent a business from routinely gathering personal information without true consent, in ways that are not otherwise reasonable under s. 11. It is designed to prevent, for example, the use of standard form contracts containing consent clauses, under the pretext that the customer is thereby "consenting" to the provision of personal information that is not reasonably necessary for the transaction.

[54] The respondent does not argue that the word "necessary" in s. 7(2) means "indispensable". He relies on previous decisions in which it was stated:

> If an organization can demonstrate that collection of personal information is necessary to enable it to meet a reasonable purpose relating to a transaction, such as to protect itself against fraud, then the collection may be a necessary condition for the purposes of s. 7(2). [Order P2007-016]

This is a reasonable interpretation. If there is a risk of fraud, it is necessary to have policies in place to prevent fraud, and to assist in the detection of those responsible when fraud occurs. So long as those necessary policies are "reasonable" they are unobjectionable. While the adjudicator adopted this definition, she did not accept that the recording of driver's licence numbers was reasonably necessary to prevent fraud.

[55] This leads to an examination of the reasonableness of the appellant's policy of collecting driver's licence numbers. More precisely, the issue is whether it was unreasonable (in the ***Dunsmuir*** sense) for the adjudicator to find that it was unreasonable (in the objective sense) for the appellant to collect these numbers as a condition of its business dealings.

[56] The adjudicator found first that the appellant was in breach of s. 11 of the *Act*:

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

She decided at paras. 22, 40:

(a) preventing fraud and theft is a reasonable purpose for collecting personal information;

(b) recording the name and address of the person picking up the furniture is reasonable;

(c) reviewing and checking a form of identification, such as a driver's licence, is reasonable;

(d) but writing down the number on the driver's licence is unreasonable.

The result is that the adjudicator concluded that the appellant's <u>purpose</u> was in compliance with s. 11(1), but its <u>means</u> of achieving the purpose was in breach of s. 11(2) insofar as it recorded the driver's licence numbers.

[57] As previously noted (*supra*, paras. 34-35 and 39), the reasonableness of the adjudicator's decision is undermined by her failure to recognize that the appellant needed to show only that its policies were "reasonable", not that they were the "best" or "least intrusive" approaches. Sections 3 and 11 do not create any test of "paramountcy"; the test is whether the use being made of the information is "reasonably necessary". That standard does not require the organization to defer in all instances to the interests of individual privacy. The respondent is not empowered to direct an organization to change the way it does business, just because the respondent thinks he has identified a better way. So long as the business is being conducted reasonably, it does not matter that there might also be other reasonable ways of conducting the business.

[58] The adjudicator reasoned at paras. 25-6 that ". . . in extremely limited factual circumstances it could be useful to record personal information of the individual picking up merchandise for the purpose of preventing fraud". She then proceeded to outline how difficult it would be for a thief to impersonate somebody and obtain merchandise by fraudulent means. She concluded that "the connection between these unlikely circumstances and the prevention of fraud is tenuous to the point of not being reasonably connected". At para. 37 she concluded that collecting licence plate numbers was pointless, because the fraudster might have been driving a borrowed car. Assuming that fraud is rare or nonexistent is contrary to common experience and common sense, and therefore unreasonable. As unlikely as it may theoretically be, the appellant has actually been the victim of such fraud. In any event, a retailer does not have to prove that fraud is commonplace, or probable, to justify having security measures in place. As long as fraud is a meaningful risk in the business, and the policies adopted have a meaningful effect on preventing or detecting fraud, those policies would be considered "appropriate in the circumstances" by reasonable people. A reasonable person would not expect a retailer to view the world through rose coloured glasses, and assume that everybody conducts themselves honestly.

[59] A good deal of argument was directed to whether the adjudicator misstated the purpose of the appellant's policy. The appellant correctly notes that the adjudicator focussed narrowly on the driver's licence policy as being directed at "preventing" fraud, whereas its primary purpose would be to protect the appellant and apprehend those responsible. The adjudicator never considered whether the appellant's policy was reasonably connected to the latter purposes. There is, however, no meaningful distinction to be made between a policy that prevents fraud and one that aids in catching those responsible. Recording the driver's licence numbers will have a general deterrent effect. If people know that there are controls in place, fewer will try to steal furniture. If there are no controls in place, the opportunistic will seek to take advantage of that opportunity. Just because the connection between the policy of recording numbers and deterring fraud is subtle and unmeasurable does not mean that it is nonexistent, tenuous or unreasonable.

[60] Deterrence is a recognized objective of many statutory regimes, and the fact that the adjudicator stated "it is unclear to me" how recording the information could prevent fraud does not make the appellant's policy unreasonable. The real point of recording the information is to be able

to locate the perpetrator if anything goes wrong. This allows the police to apprehend whoever is responsible, but it also allows the appellant to protect itself from claims by its customer. If the customer is complicit in the fraud, it allows the appellant to demonstrate that authorized persons did in fact pick up the furniture. Recovering the balance owing for goods sold on credit would require the appellant to prove delivery to an authorized person. Merchandise cannot be delivered to the right person if it has already been delivered to the wrong person, making the prevention of delivery to the wrong person strictly and literally "necessary" to supply the product or service to the right person. The policy protects customers whose identity information has been lost or compromised. The reasonable person would regard the appellant's practices as being reasonably necessary in the circumstances.

[61] It was not unreasonable for the appellant to conclude that the adjudicator's solution of just writing down the name and address on the driver's licence was inadequate, because common names are indistinguishable, and the address may be out of date. A good illustration of the reasonableness of also recording the number is found in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184, s. 67(a). It is statutory recognition that there is incremental value in recording an identification number along with the name by requiring a financial institution to record, in addition to the name of the person, ". . . if a birth certificate, driver's licence, provincial health insurance card . . . , passport or any other similar record is relied on to ascertain the person's identity, the type and reference number of the record and the place where it was issued". Requiring the production of the driver's licence is a reasonable way of preventing a fraudster from just (falsely) giving the name of the customer; it provides one further level of security. Going another step, and writing down the driver's licence number involves no meaningful further intrusion on the customer's privacy, nor increase in risk of the misuse of the customer's personal information. Also recording the vehicle licence plate number creates another obstacle for the fraudster, as it provides a second avenue of inquiry. Assuming the information is properly stored (and, again, the appellant's practices in this regard were not in issue), the added risk is small, as the name and address themselves can be used for illegitimate purposes.

[62] The conclusion that it was reasonable to check identification, but not to record the number would not be considered appropriate by reasonable people. Any large organization needs to keep records for information to be of any use. The personnel on the loading dock undoubtedly perform many identification checks every month, and it is unrealistic to think that they can remember one customer from the other. If someone ever did fraudulently pick up furniture, how could the personnel ever remember who it was, what the circumstances were, and what type of identification was provided if no record is kept? Without a record of the number, how could the personnel provide any useful information to the police who are investigating? Even if the fraudster was driving a borrowed car, having the licence plate number would be valuable information for the police in tracing the culprit. How that information is stored, and the length of time it is held are different matters, but merely recording the identification information is a reasonable and, indeed, sensible practice. Section 17(d) authorizes the use of personal information for just this purpose: "the use of

the information is reasonable for the purposes of an investigation or a legal proceeding". If the appellant is allowed to use it, implicitly it must be able to collect it. The adjudicator's finding to the contrary is not one reasonably open on the facts and the law.

[63] The adjudicator observed at paras. 32, 34 that driver's licence numbers are sensitive and valuable data that can be misused if they fall into the wrong hands. The appellant was not, however, charged or investigated with respect to the security of its storage of those numbers, nor with respect to its policies respecting retention or use of the numbers. Those are discrete issues that are not dealt with in this appeal. The only issue presently before the Court concerns the right of the appellant to record the numbers.

[64] The respondent argues that the recording of driver's licence numbers should be strictly controlled, because they can be used to locate other sensitive information about the driver. But that is true of any form of identification. The whole point of identification is that it can be used to identify. Similar arguments can be made about the name of any person: one's name can obviously be used to trace other personal information about the person, yet no one would suggest that we stop using our names. The *Act* recognizes that the reasonable use of personal information is legitimate, and does not mandate "strict control" of such information.

[65] In summary, the adjudicator's conclusion that the respondent's policy on the delivery of goods to third parties was unreasonable is itself unreasonable. It is not one of the solutions that are available on the facts and the law. The adjudicator's approach was influenced by the view that privacy rights prevail in all circumstances over the legitimate need to use information. It was also unreasonable for the adjudicator to conclude that the appellant's policy was unreasonable, because the adjudicator thought that there were other reasonable ways that the business could be operated.

<u>Failing to Communicate its Policy</u>

[66] The adjudicator also found the appellant to be in breach of s. 13 of the *Act*:

> 13(1) Before or at the time of collecting personal information about an individual from the individual, 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.

The staff on the loading dock were only able to tell the customer's mother that the information was being collected because it was "store policy". The adjudicator found this to be inadequate. Since the adjudicator granted no remedy with respect to this breach, the issue is moot and no further discussion is warranted.

Conclusion

[67] In conclusion, having regard to both her reasons and to the eventual outcome, the decision of the adjudicator is unreasonable. Even extending appropriate deference to the adjudicator in her interpretation of the statute, and its application to the facts, the decision does not fall within a range of possible, acceptable outcomes which are defensible in respect of the facts and law. The statute calls for a balancing of interests, and the adjudicator did no balancing. The premise underlying much of the reasoning (that privacy rights must always prevail over the reasonable use of information) is not one that is available on a reasonable interpretation of the statute. The adjudicator also failed to realize that the presence of other reasonable methods of conducting the appellant's business does not mean that the appellant's chosen method is unreasonable. The appeal from the order of the chambers judge is allowed, and the decision is quashed.

Appeal heard on September 16, 2010

Reasons filed at Calgary, Alberta
this 28th day of March, 2011

Slatter J.A.

I concur:
Authorized to sign for: Berger J.A.

Dissenting Reasons for Judgment Reserved of
The Honourable Madam Justice Conrad

I. Introduction

[68] This appeal is about personal privacy and the extent to which the *Personal Information Protection Act*, SA 2003, c P-6.5 (*PIPA*) limits a retailer's right to retain information about an individual. In particular, this case deals with the meaning of "personal information", under section 1(k) of *PIPA*, and the statutory limitations imposed on the collection and retention of an individual's driver's licence number and the motor vehicle licence number of the vehicle used to pick up furniture.

II. Issues

[69] Leon's Furniture Limited (Leon's) appeals the dismissal of an application for judicial review of a decision of an adjudicator from the office of Alberta's Information and Privacy Commissioner (Commissioner). The appellant argued before the chambers judge, and reiterates here, that the adjudicator came to an unreasonable decision by:

(a) concluding that drivers' licence numbers and vehicle licence plate numbers are "personal information within the meaning of the Act";

(b) misapprehending or misstating the purpose of the Pick Up Sales Policy;

(c) failing to undertake a balancing of interests as mandated by *PIPA*; and

(d) unreasonably failing to address the mischief targeted by *PIPA*, namely, identity theft and intrusive marketing activity.

III. Decision

[70] The appeal is dismissed. The reviewing judge selected the proper standard of review – reasonableness. She considered Leon's arguments carefully and determined that the adjudicator's decision on each ground was reasonable in the sense that the decision fell within a reasonable range of outcomes. The reviewing judge did not err. The adjudicator's decision was reasonable and it is owed deference.

IV. Background

[71] Leon's is a retail supplier of furniture, appliances and electronics. Goods purchased from Leon's are often picked up at a date subsequent to the date of purchase, and occasionally the pick up is performed by third parties. To protect itself and its customers from fraudulent pick ups, in such cases Leon's has adopted a written policy requiring persons picking up goods to present an acceptable form of identification, one of which could be a driver's licence. The name of the person picking up the furniture is recorded on the sales slip.

[72] Supplemental to this written policy, however, Leon's has adopted the practice of recording the driver's licence number of the person picking up the goods, as well as the vehicle licence number of the automobile being used for the pick up. Thus, when the pick up person appears, his or her identity is confirmed as being the person authorized to pick up the goods. The person's driver's licence number is then recorded on an internal document called a "pick ticket" which is retained and filed separate from the sales slip. Although the pick ticket was not entered in evidence in the proceeding before the adjudicator, the adjudicator accepted Leon's statement that the recipient's name is not normally recorded on the pick ticket. The adjudicator also found that for the pick ticket to be meaningful there had to have been a means of relating it to the sales receipt. She drew the inference, therefore, that the invoice number (or some other reference) would be recorded on the pick ticket enabling it to be linked back to the sales order containing the recipient's name.

[73] The present appeal arises from a complaint filed by Sharon Curtis – the complainant. On December 26, 2006, the complainant's daughter ordered a table from Leon's and paid a deposit. She indicated that her mother, the complainant, would be picking up the table when it arrived. The complainant's name was recorded on the sales slip. The sales slip also noted that identification would be required on pick up.

[74] On January 30, 2007, the complainant attended at Leon's to pick up the table. She paid the balance owing on the furniture with a credit card. The sales clerk requested further identification and the complainant offered various cards but the clerk insisted on a driver's licence. The complainant then produced her driver's licence and the clerk recorded the driver's licence number from it on the pick ticket. The complainant did not want her number recorded. When she asked why this was being done, the sales clerk replied that store policy required her to do this.

[75] The complainant was then escorted to the pick up area where the sales slip was handed to another staff member. That staff member asked the complainant to sign an acknowledgment that she had received the furniture and directed that she write her licence plate number on the acknowledgment. Again the complainant objected, but under the impression this was the only way to obtain the furniture, she complied. According to Leon's, this information was recorded on another pick ticket and stored.

[76] On February 6, 2007, the complainant wrote to the Commissioner's office complaining about the recording and retention of her driver's licence number, and vehicle licence number. Among other things, she stated:

> I am uncomfortable that they have so much of my personal information recorded and would like to know if they have a right to gather & keep that information and what they might be using it for, ie: passing it on for any purposes, selling my information, etc. I am also concerned about the level [of] security in their information system, given the recent breach of security in the Winner's and Home Sense situation.

[77] The Commissioner's office issued a Notice of Inquiry on April 22, 2008, asking the parties to address whether the information collected was "personal information" under *PIPA* and, if so, whether by collecting the complainant's personal information, in the way that it did, Leon's had breached sections 11, 7(2) and 13. Submissions from both parties were subsequently filed and exchanged.

V. The Adjudicator's Decision

[78] An adjudicator from the Commissioner's office dealt with the complaint. The adjudicator found, as a threshold issue, that the complainant's driver's licence number, and her vehicle licence plate number constituted "personal information" under *PIPA*. The adjudicator then proceeded to determine whether the specific provisions of *PIPA* had been breached.

[79] She first considered whether Leon's had complied with the general limitation on collecting personal information set out in section 11 of *PIPA*. Leon's had argued that the purpose of collecting driver's licence information, and vehicle licence numbers, was to assist the customer, the police and the company in the event of fraud, as well as to prevent fraud. The adjudicator concluded that while preventing fraud might be a reasonable purpose under section 11(1), Leon's current policy breached section 11(2) because it went beyond what was reasonable for meeting the purposes for which the information was collected, and was not reasonably connected to the purposes of the collection. While acknowledging that retaining the name and address of an individual picking up the furniture would be reasonable, retaining her driver's licence number and vehicle plate number went beyond what was reasonable for meeting the accepted purpose.

[80] In relation to this breach, she determined that Leon's did not even follow its own policy. The written policy provided for many acceptable types of identification such as "Drivers Licence, Health Card with photo, Passport, Native Status Card, Canadian Citizenship Card, Senior Citizens Card, Military identification with photo, Fire Arms Registration Card and Valid Major Credit Card (Visa, Master Card or American Express)". Licence plates were not listed.

[81] The adjudicator then turned to the issue of whether either the driver's licence or the licence plate numbers had been obtained without the complainant's consent. First, she reviewed section 7(2) of *PIPA* and found Leon's had breached the section by making consent to the collection of personal information a condition of the pick up when this was not necessary to provide the product or service. Then she turned to section 13 of *PIPA* and concluded that Leon's had breached that section by failing to explain the purpose of the collection policy adequately to the complainant, and by failing to properly identify a person in the organization who could answer the complainant's questions about the collection.

[82] Having found these breaches of *PIPA*, and pursuant to her authority under section 52 of *PIPA,* the adjudicator ordered Leon's to cease collecting this information and to destroy all such information in its possession. Leon's response was to bring an application for judicial review.

VI. The Decision of the Reviewing Judge

[83] The issues argued in the judicial review application were the same as the grounds of appeal set out above. The parties agreed that the standard of review on all issues was reasonableness. After considering the appellant's arguments, the reviewing judge concluded that the adjudicator had fully understood Leon's arguments, that she had been alive to the issues, and that her conclusions on each issue fell within a range of reasonable outcomes. As a result, the standard of review precluded interference and the reviewing judge dismissed the application for judicial review.

VII. Standard of Review

[84] The parties agree that the reviewing judge's decision must be correct, both with respect to the choice of the standard of review and its application. Similarly, they agree that the standard the reviewing judge was bound to apply to the adjudicator's decision was one of reasonableness. This standard was described by the Supreme Court in *Dunsmuir v New Brunswick*, 2008 SCC 9 at para 47, [2008] 1 SCR 190 in the following way:

> A court conducting a review for reasonableness inquires into the qualities that make a decision reasonable, referring both to the process of articulating the reasons and to outcomes. In judicial review, reasonableness is concerned mostly with the existence of justification, transparency and intelligibility within the decision-making process. But it is also concerned with whether the decision falls within a range of possible, acceptable outcomes which are defensible in respect of the facts and law.

[85] I agree with the way the parties have formulated the standard of review. There being no issue as to whether the reviewing judge chose the correct standard of review, the sole issue is whether the

reviewing judge erred when she concluded that the adjudicator's decision with respect to each of the four grounds of review was reasonable.

VIII. Standing

[86] I agree with my colleague's conclusion that in the particular circumstances of this case, where the complainant's side is otherwise unrepresented, the Commissioner has standing on appeal.

IX. Analysis

A. The statutory scheme

[87] Before setting out the statutory scheme in detail it is necessary to make a few comments about the purpose behind the statute.[1] Advances in technology have made it possible for organizations to accumulate a great deal of information about an individual. In this case, for example, in the course of the transaction, Leon's had access to the complainant's name, her address, her credit card information, her driver's licence number, her vehicle licence number, as well as her daughter's name, address, and credit information. But data like this, when aggregated, can easily be misused or misappropriated. At the very least, it may result in unwanted marketing and solicitation, particularly when the personal information is shared with other organizations. In the worst case, it may lead to significant crimes such as identity theft.

[88] A good example of the dangers inherent in the collection of personal information by organizations is found in the facts behind the *Report of an Investigation into the Security, Collection and Retention of Personal Information, September 24, 2007, TJX Companies Inc/Winners Merchant International LP*, P2007-IR-006 (*Winners*), a joint report of the Privacy Commissioners of Canada and Alberta which was discussed and applied by the adjudicator in the present case. Winners – a well-known retailer – was in the habit of collecting and storing a great deal of client personal information in the course of its business. Starting in 2005, and continuing at intervals into 2007, Winners' computer system was compromised by intruders who gained access to much of this information and appropriated it for illegal purposes.

[89] Personal privacy is an important social value that is being significantly eroded in this way. It is easy to comprehend the wrong when an organization sells or trades an individual's personal information. But it is important to recognize that the starting point for the potential misuse of such data begins with its collection. Prior to the enactment of *PIPA* in 2003, there was no restriction on an organization's ability to collect, use and distribute personal information. The Legislature, however, recognizing the dangers associated with these activities, enacted *PIPA* to balance an

---

[1] Statutory references are to *PIPA*, as it existed, in 2008.

individual's right to keep personal information private against an organization's legitimate need for such information. Thus, section 3 describes the overall purpose of the statute in the following way:

> 3. The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.

[90] The definition of "personal information" is found in section 1(k):

> "personal information" means information about an identifiable individual;

[91] To balance the right of an individual to keep his personal information private, against the needs of the organization, the statute sets out a scheme by proscribing, absolutely, the collection, use and disclosure of personal information – unless certain conditions are met or certain exemptions apply. The first condition is consent. Section 7(1) sets out this general requirement:

> 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,
>
> (c) use that information unless the individual consents to the use of that information, or
>
> (d) disclose that information unless the individual consents to the disclosure of that information.

[92] If consent is demanded as a condition of supplying a service or product, section 7(2) makes clear that consent can only be extracted in this fashion to the point that it is "necessary" to provide the product or service. The section reads:

> (2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure

> of personal information about an individual beyond what is necessary to provide the product or service.

[93] There are exceptions to the general requirement of consent set out elsewhere in *PIPA*. As this appeal deals with the "collection" of personal information it is necessary to refer to sections 14 and 15 of the statute. Section 14 describes the general situations where personal information can be collected without consent. The opening words make clear that these are the only exceptions. The words read:

> 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**... [emphasis added]

[94] Section 15 deals specifically with the collection of personal information in the employment setting and indicates that slightly different rules apply in that context. Its opening words – "Notwithstanding anything in this Act other than subsection (2)..." – indicate it is intended as a single exception to the exclusivity of section 14.

[95] Section 8 of the legislation indicates that consent can be in writing or oral, and consent may be deemed to have been given where the information is submitted voluntarily and it is reasonable for the person to have given the information voluntarily. Sections 8(1) and 8(2) read:

> 8(1) An individual may give his or her consent in writing or orally to the collection, use or disclosure of personal information about the individual.
>
> (2) An individual is deemed to consent to the collection, use or disclosure of personal information about the individual by an organization for a particular purpose if
>
> (a) the individual, without actually giving a consent referred to in subsection (1), voluntarily provides the information to the organization for that purpose, **and**
>
> (b) it is reasonable that a person would voluntarily provide that information. [emphasis added]

[96] A further form of deemed consent is found in section 8(3) which allows an organization to collect, use and disclose personal information where it has given an individual notice of its intention to collect information, and given the individual a reasonable opportunity to decline, and there has been no response.

[97] Section 11 places yet another limitation on the collection, use and disclosure of personal information even where consent has been properly obtained or deemed, or where it is not necessary to obtain consent. Section 11 provides:

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

[98] Finally, section 13 is also relevant to the collection of personal information. It stipulates that before an organization can collect personal information, even with consent, for a reasonable purpose, and only to the extent that it is reasonable to meet that purpose, it must give notice. The section reads:

> 13 (1) Before or at the time of collecting personal information about an individual from the individual, 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 of a person who is able to answer on behalf of the organization the individual's questions about the collection.

(The requirements of section 13 do not apply to deemed consent under section 8(3): see section 13(4)).

[99] In summary, the Legislature has chosen to balance the individual's right to privacy against the needs of an organization by the following scheme:

1. Organizations are prohibited from collecting personal information without an individual's consent, unless the information falls within an exception specifically provided in sections 14 and 15.

2. Organizations cannot require consent to the collection of personal information as a condition of supplying a service or product unless the collection is **necessary to provide the product or service.** Necessity becomes the only basis for making consent a condition of the provision of a service or product.

3. Consent can be oral or in writing and can be deemed where the conditions in section 8 are met.

4. Even where an individual consents or is deemed to have consented to the collection of personal information, or where consent is unnecessary under section 14, an organization can only collect information **for purposes that are reasonable, and then only to the extent that is reasonable for meeting that purpose**. Section 11 is not an exception to obtaining consent. Rather, as both parties acknowledged in supplemental argument, even when a person freely consents to the collection of information, organizations are prohibited from collecting it unless section 11 is satisfied. Were this not the case, there would be no incentive to obtain consent and organizations would simply rely on section 11. Sections 7 and 14 would, in large part, be unnecessary.

5. Consent, when obtained, must be informed. An organization must notify the individual whose personal information is being collected why collection is necessary and who, within the organization, has been delegated to answer questions about the collection.

[100] With these principles in mind, I turn to the issues raised on appeal.

B. Issue One – Was the adjudicator's determination that driver's licence numbers and licence plate numbers are "personal information" reasonable?

[101] Leon's submits that neither the complainant's driver's licence number, nor her vehicle licence plate number, amount to "personal information" as neither is "information about an identifiable individual" as described by section 1(k) of *PIPA*. In support of this argument, Leon's says that the legislative intent is to proscribe the collection of information about an individual that is personal – such as taste, personal style or personal intentions – and gives rise to a reasonable expectation of privacy. In Leon's view, neither a driver's licence number, nor a vehicle plate number, disclose this kind of information. Moreover, Leon's says that the information is not about an identifiable person because the complainant's name was not stored on the same document as either the driver's licence number or plate number. Therefore, her identity could not be ascertained without reference to access-restricted government databases. As a result, Leon's says that the adjudicator's findings are unreasonable.

[102] To assess the merit of Leon's submissions, it is necessary to examine the definition of "personal information" under *PIPA*. Unfortunately, there is little judicial authority interpreting the meaning of "information about an identifiable individual" in privacy legislation such as *PIPA* which regulates the relationship between individuals and private organizations. These words have been interpreted with respect to privacy legislation, however, which regulates the use and disclosure of

personal information by public bodies. While the interests being balanced in such legislation are not identical to those being balanced in legislation dealing with private organizations, they are similar, with the result that the authorities interpreting such legislation are relevant and helpful.

[103] The words "information about an identifiable individual," for example, are found in section 3 of the federal *Privacy Act*, RSC 1985, c P-21 (*Privacy Act*) and were interpreted by the Supreme Court of Canada in *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403, 148 DLR (4th) 385. In that case, the issue was whether sign-in logs used at the Ministry of Finance amounted to personal information and were thus protected from disclosure under freedom of information legislation. The log information was collected for a period of a month to determine week-end use for fire and emergency purposes.

[104] As the identity of employees was disclosed in the logs, there was no dispute that the information related to identifiable individuals. The sole question was whether the information found in the logs was information "about" those individuals. Speaking for the entire court on this point, LaForest J adopted a broad approach to the scope of personal information in privacy legislation. He found that the section was designed to capture any information about a particular person, subject only to specific exceptions found in the *Privacy Act*. He stated at paras 68-69:

> In its opening paragraph, the provision states that "personal information" means "information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing". On a plain reading, this definition is **undeniably expansive**. ...
>
> As noted by Jerome A.C.J. in *Canada (Information Commissioner) v. Canada (Solicitor General), supra*, at p. 557, the language of this section is "deliberately broad" and "entirely consistent with the great pains that have been taken to safeguard individual identity". **Its intent seems to be to capture any information about a specific person, subject only to specific exceptions;** see J. Alan Leadbeater, "How Much Privacy for Public Officials?", speech to Canadian Bar Association (Ontario), March 25, 1994, at p. 17. Such an interpretation accords with the plain language of the statute, its legislative history and the privileged, foundational position of privacy interests in our social and legal culture. [emphasis added]

[105] His Lordship went on to conclude that because the information requested described the times during which employees of the Department of Finance attended the workplace on weekends it amounted to information about those employees and was, *prima facie*, personal information about them. This same broad definition was later applied by the court to the employment records of four police officers in *Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8, [2003] 1 SCR 66.

[106] The Ontario courts have also interpreted the phrase "information about an identifiable individual", as found in Ontario's *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F31, and concluded that a broad interpretation is required. In *Ontario (Attorney General) v Ontario (Information and Privacy Commissioner)* (2001), 154 OAC 97, 16 CPR (4th) 460 (ONSC Div Ct), (aff'd *Ontario (Attorney General) v Pascoe* (2002), 166 OAC 88, 22 CPR (4th) 447 (Ont CA)), the Ontario Superior Court of Justice (Divisional Court) considered whether doctors' billing information qualified as "information about an identifiable individual". The question in the case was not whether billing information was information "about" a doctor. Rather, the issue related to whether individual doctors could be identified from the information so that the information amounted, in each case, to information about an identifiable individual. In this context, the court held that any information which, when combined with other information, could identify a person, amounted to information about an identifiable individual under the statute. The court stated at paras 14-15:

> While the records in question do not name the physician, it is common ground that the records may themselves, or in combination with other information, identify the individual even if he or she is not specifically named. The test is accepted as follows:
>
> > "If there is a reasonable expectation that the individual can be identified from the information, then such information qualifies under subs. 2(1) as personal information." Order P-230, [1991] O.I.P.C. No. 21.
>
> The test then for whether a record can give personal information asks if there is a reasonable expectation that, when the information in it is combined with information from other sources otherwise available, the individual can be identified. A person is also identifiable from a record where he or she could be identified by those familiar with the particular circumstances or events contained in the record. See Order P-316, [1992] O.I.P.C. No. 74; and Order P-651, [1994] O.I.P.C. No. 104. [emphasis added]

[107] Yamauchi J came to a similar conclusion in *University of Alberta v Alberta (Information and Privacy Commissioner)*, 2009 ABQB 112, 470 AR 72. In that case, a university professor objected to the publication of statistical employment information concerning teaching effectiveness, the number of published papers and merit increase recommendations regarding members of the faculty of Electrical and Computer Engineering. The professor argued that the information was displayed in such a way that anyone reviewing the published material could tell what parts of it referred to him. It followed, therefore, that the information, which concerned his effectiveness as a teacher and scholar, was "information about an identifiable individual" under Alberta's *Freedom of Information*

and Protection of Privacy Act, RSA 2000, c F-25 which could not be disclosed without his consent. An adjudicator from the Privacy Commissioner's office agreed with him and the University sought judicial review.

[108] The reviewing judge found, given the nature of the information in dispute, that if the complainant could be identified from the information he was an identifiable individual under the definition of personal information. He stated at para 64 of his reasons:

> If one could glean personal information from the numerical information, however, that alone would be a disclosure of personal information. As stated in *Human Resources* at para. 21:
>
> > ... it is not necessary to specifically name employees for there to be recorded information about an identifiable individual. Facts and event, the context in which information is given, as well as the nature and content of the information may also be personal information if it is shown to be recorded information about an identifiable individual. The key here is whether there is an "identifiable" individual.

[109] The Federal Court of Appeal has also interpreted the phrase "information about an identifiable individual," as found in the federal *Privacy Act*. In *Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board*), 2006 FCA 157, [2007] 1 FCR 203, the Canadian Transport Accident Investigation Commission and Safety Board refused to release information regarding four air occurrences that had been investigated because it would involve the release of personal information. The court accepted the logic of the Ontario courts with respect to the concept of an "identifiable individual", suggesting the words implied "someone whom it is reasonable to expect can be identified from the information in issue when combined with information from sources otherwise available" (para 43). It took a narrower view, however, of the words "information about" than that taken by LaForest J in *Dagg*. The Federal Court held that once an individual was identified, or found to be identifiable, there was still a requirement that the information being sought had to be sufficiently connected to the individual to provoke an expectation that the information would be kept private. In coming to this conclusion, the court relied, in part, on *dicta* from LaForest J's decision in *Dagg* discussing the search and seizure cases under the *Charter of Rights and Freedoms*.

[110] While I agree with the Federal Court that the phrase "information about an identifiable individual" requires two discrete inquiries – is there information "about" an individual, and can that individual be identified – I do not accept that the concept of personal information is as narrow as suggested. The Supreme Court made clear in *Dagg* that the test to be applied is a broad one, and that personal information includes "any information about a specific person" provided that person can

be identified. Thus, provided the information discloses something about an identifiable individual it amounts to personal information.

[111] Furthermore, I do not find the search and seizure cases useful in understanding the meaning of personal information as found in privacy legislation. The comments relied upon by the Federal Court of Appeal were clearly *dicta*. Having already determined that the phrase "information about an individual" meant any information about that individual, LaForest J simply went on to discuss the narrower test employed in the search and seizure cases under the *Charter of Rights and Freedoms*. He found that an application of the stricter test employed in the search and seizure cases would also have been satisfied on the facts of *Dagg*. But he noted, at para 70, that this was "not strictly necessary" to his analysis, as he had already defined personal information broadly. In my view, therefore, the Federal Court's reliance on comments relating to application of the search and seizure test failed to appreciate that Laforest J had already set a broader test for privacy legislation of this type.

[112] Moreover, while the concept of a "reasonable expectation of privacy" may be useful in describing the zone into which the police cannot intrude without reasonable and probable grounds, it does not assist in the interpretation of statutes such as *PIPA*, which are concerned with controlling the collection, use and distribution of an individual's personal information in the world of private commerce. *PIPA* does not purport to describe a protected zone of privacy into which the state cannot intrude. Nor does it seek to protect personal information of all kinds from all persons. Rather, the statute protects the collection, use and transmission of personal information about an individual where such collection, use or transmission is not reasonably necessary. It is legislation aimed at curbing abuses with respect to such information in the world of commerce. The distinction between these two strategies was noted by Colin H.H. McNairn and Alexander K. Scott in their text on *Privacy Law in Canada* (Markham: Butterworths, 2001) at 2-3:

> Lawmakers – legislators, judges, and administrative tribunals – have generally taken the broad privacy-protection approach in the tort and employment law areas. ... These statutes do not generally define precisely what territory privacy covers. ... In these areas, Canadian lawmakers have chosen to protect privacy as such, but without the benefit of any precise working definition of the term.
>
> ...
>
> In other areas, Canadian lawmakers have focused on personal information protection. Instead of protecting privacy *per se*, they have opted to take on the seemingly more modest goal of controlling the collection, use, and disclosure of such information. The most striking example of this approach is found in the recently enacted *Personal Information Protection and Electronic Documents Act*.

[113] Alberta's *PIPA* is closely modelled after the federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (*PIPEDA*). The strategy in both acts is to protect privacy by giving individuals more control over the collection of any and all information about them, and ensuring that such information is only collected, used, and disclosed by private organizations where reasonably necessary. It is aimed at limiting unnecessary data aggregation. This is a different approach than deciding first what information is intended to be kept private and then restricting the distribution of that information. *PIPA* is not concerned with whether the information was made in the expectation of privacy. Rather, *PIPA* is aimed at curbing the collection, use and disclosure of information about identifiable persons, in the hopes of preventing identity theft and curbing any misuse of information about the citizens of Alberta. Limiting misuse starts with limits on the collection of personal information. Although *PIPA* involves a balancing of interests, they are different interests than those involved in balancing the rights of citizens to be free from intrusions by the state.

[114] In my view, therefore, the following principles can be gleaned from the authorities regarding the interpretation of the words "information about an identifiable individual" found in section 1(k) of *PIPA*:

1. The words used are deliberately expansive and must be interpreted broadly: (*Dagg*; *(Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police)*). The words "information about" describe **any information** "about" an identifiable individual and not just information an individual would "reasonably expect" to keep private.

2. The statute speaks of an "identifiable individual" not an "identified individual". Thus, the information must be about a person who is known or can be identified either from the information itself, or when that information is combined with other information: (*Pascoe*; *University of Alberta v Alberta (Information and Privacy Commissioner); Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)*)

[115] I turn to the issue of whether it was reasonable for the adjudicator to conclude that the complainant's driver's licence number and vehicle licence number amounted to "personal information". To make this assessment, the adjudicator was obliged to determine whether either of these numbers revealed information "about" an individual, and whether that individual was identifiable. While she did not conduct two discrete enquiries, she found, nonetheless, that both criteria were met. She stated at paras 12-13:

> While it is true that every individual could not look at drivers' license numbers and know whose license it is, drivers' license numbers alone are

> still information about an identifiable individual. It is a unique number assigned to an individual. When searched using the appropriate database, it can easily be connected to a name, birth date, physical description and various other pieces of personal information. The same would be true of a license plate number, which, if searched, would reveal personal information about the person to whom the license plate number is registered.
>
> I was not provided with a copy of the pick tickets by the Organization as part of its submission. The Organization did advise that it collected this information which the organization believes is only usable by the police should a fraud investigation become necessary. Presumably, in order to make this information useful if necessary, there would have to be some way of searching it. Although the Complainant's name was not recorded on the pick tickets, presumably the invoice number for the sale was. This number could then lead the Organization back to the Sales Receipt and Sales Order which does have the Complainant's name on it. If the person picking up the merchandise was the customer, the pick ticket could link back to the sales order and receipt which contain the customer's name and address.

[116] Were these conclusions reasonable? Dealing first with the adjudicator's decision about the driver's licence number, the adjudicator found that the number amounted to information about an individual because it could lead to further information about the licence holder, such as his or her age, address and physical description, when searched in the appropriate database. I agree. Indeed, I would have gone further and found that a person's driver's licence number is, by itself, "information about" that person. In simple terms, just as a person has a certain eye and hair colour, a person has a driver's licence number. The significance of the number is demonstrated by the fact that driver's licence numbers are often sought by rogues and fraud artists wishing to steal a person's identity. It is exactly the type of information the statute seeks to prevent organizations from collecting unnecessarily. A driver's licence number is private information about an individual because of what it represents and what it can be used for. The privacy of this information must be guarded sedulously.

[117] The adjudicator also found that the information concerned an identifiable individual. She did this in two ways. First, she assumed that a means must exist by which the organization could associate the name of the person picking up the purchased item with the driver's licence number. She reasoned, therefore, that as Leon's would want to track the licence number back to the sales slip, which contained the complainant's name, the pick tickets must have contained a reference to the invoice. As Leon's did not supply the pick ticket to the adjudicator, she was entitled to draw this inference. Second, the adjudicator found that even without cross-referencing the pick ticket to the sales receipt, the complainant's identity could be ascertained by searching the appropriate database. This, too, was a reasonable conclusion because as long as the complainant could have been

identified through the information collected, "when combined with information from other sources," this was enough to satisfy the requirement that an individual be identifiable would be satisfied: *Pascoe*; *Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)*.

[118] In my view, the adjudicator's conclusion that the complainant's driver's licence number amounted to "personal information" was well within "the range of acceptable outcomes which are defensible in respect of the facts and law." It was reasonable and there is no basis for interference.

[119] The same is true of the adjudicator's decision with respect to the complainant's vehicle licence number. The question of whether a motor vehicle licence number in this case is personal information is not as clear with a driver's licence number. While it is suggested that a licence plate number is information about an automobile rather than an individual, the licence plate number, as the adjudicator noted, when searched in the appropriate database, also produces information about the owner which in the vast majority of cases will be the person picking up the item. Furthermore, I am satisfied that even where the pick up person is not the owner, the type of car a person drives is information about that individual's choices and status in life. This is so whether that car is owned, rented, leased or borrowed. A licence plate number of a car driven by an individual is, therefore, information about that individual, despite also being information about the automobile to which it is attached, the province in which it is registered, and innumerable other things.

[120] Much was made at the appeal hearing about licence plate numbers and the fact that they are publicly displayed. It was argued that because anyone can copy down a licence plate number, these numbers cannot amount to personal information about an individual as there is no expectation of privacy concerning them. But, as discussed above, this legislation is not designed to protect an expectation of privacy. Nor is it designed to protect against the collection, use and disclosure of personal information by one's neighbour. It is aimed at organizations. *PIPA* is the Legislature's acknowledgment that the use of modern technology in commerce has made vast quantities of personal information publicly available, and while it is impossible to regulate the flow of information about individuals completely, it is possible to control its collection, use and disclosure by organizations. Every datum centralized in one locale increases the ease of targeting an individual for mass marketing or identity theft.

[121] Therefore, the fact that a licence plate number is openly displayed, for ease of law enforcement, is not determinative when it comes to deciding whether it is personal information, or whether an organization is entitled to collect, use and distribute it. More importantly, perhaps, and as the adjudicator found, even though the vehicle licence number itself is publicly displayed, the number is merely a conduit to other personal information about the owner that is not publicly available (see Alta Reg 140/2003, *Access to Motor Vehicle Information Regulation*).

[122] I would add, with respect to both numbers, that Leon's wanted to collect them precisely because they could lead to personal information about the complainant. Leon's cannot now be heard to say that the numbers did not disclose personal information when the whole reason behind their collection was to establish a path to the complainant in the event of fraud.

[123] In summary, the adjudicator's conclusion that both licence numbers were personal information under *PIPA* was reasonable and the reviewing judge correctly afforded that decision deference.

C. Issue Two – Did the Commissioner mis-state or misapprehend the purpose of the pick-up sales policy?

[124] Leon's submits that although the adjudicator correctly found that the purpose of the policy was to assist Leon's customers and the police once fraud had been committed, she applied the policy as if its purpose was the prevention of fraud when assessing the reasonableness of the policy under sections 11(2) and 7(2) of *PIPA*. Leon's submits that by converting the purpose of the policy into the prevention of fraud the adjudicator set up a "straw man", and that if she had assessed the policy in light of the purpose first identified she would have come to a different conclusion.

[125] In my view, there is no merit to this argument. I agree with my colleague that there is no meaningful distinction to be made between a policy that prevents fraud and one that aids in catching those responsible for it. In any event, as the reviewing judge noted, the adjudicator was fully alive to all of Leon's arguments and its reasons for collecting the licence numbers. She understood that the collection of the complainant's personal information was designed to assist Leon's, its customers and the police in the event of fraud, and the adjudicator's reference to fraud prevention does not alter that fact. Furthermore, even Leon's referred to fraud prevention as part of the reason for the policy. As the adjudicator noted at paras 19-20 of her reasons:

> The Organization provided me with a revised procedure memo dated June 1, 2004 ("written policy memo") which states that **in order to prevent incidences of fraud**, when items are being picked up after the date of purchase, identification is required. This is reasonable, as the sales employee may not have been the employee that rang in the original sale and therefore **confirming the identity of the individual picking up the item is a reasonable way of preventing fraud in this situation**.
> Further, the Organization argues that by collecting only drivers' license numbers and not the names and addresses of those picking up the merchandise, **it has chosen the safest means of preventing fraud**. [emphasis added]

[126] Thus, a fair reading of the adjudicator's reasons reveals that she understood the appellant's argument. She understood that the policy was designed to protect Leon's and its customers in the event of a wrongful pick up. She did not act unreasonably in considering the purpose of preventing fraud in assessing whether Leon's policy was reasonable for the purposes of section 11(2) of *PIPA*, or whether it went "beyond" what was required for purposes of section 7(2). The reviewing judge correctly dismissed this ground of review.

D. Issue Three – Did the Commissioner fail to undertake the balancing mandated by section 3 of *PIPA*?

[127] Leon's submits that once the adjudicator determined that individual sections of *PIPA* had been breached she was then obliged to conduct a balancing under section 3. This section reads:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.

[128] As I have already discussed, at some length above, section 3 sets out the statute's purpose, and the remainder of the statute describes the means of accomplishing it. Here the Legislature has chosen to balance the interests described in section 3 by proscribing, *inter alia*, the collection of personal information without consent, actual or deemed, subject to certain specified exceptions. Furthermore, even where informed consent is provided, the Legislature has provided a limitation to collection, found in section 7(2) which was held to have been breached in this case. That section reads:

> 7(2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual **beyond what is necessary** to provide the product or service. [emphasis added]

[129] Finally, even where there is consent, or consent is unnecessary, the Legislature has created a further limitation found in section 11, which was also held to have been breached in this case. That section reads:

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

> (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. [emphasis added]

[130] Thus, while the statement of purpose found in section 3 informs the statute's interpretation, neither section 3, nor any other section, prescribes a balancing procedure that must take place separate and apart from what is found in other sections of the *Act*. The scheme for achieving the legislative purpose is set out in the statute and that scheme governs. That scheme prohibits the collection, use and disclosure of personal information unless certain criteria are met. This is the means the Legislature has chosen to achieve the purpose set out in section 3.

[131] Furthermore, I am satisfied that the adjudicator did not come to an unreasonable conclusion in her interpretation and application of these sections. It might have been preferable for the adjudicator to start with the issue of consent, and whether it was properly given or required, as section 11 is the last hurdle an organization must overcome to justify the collection of personal information. Nevertheless, the adjudicator began her analysis by looking at section 11 to determine whether the complainant's personal information was being collected for a reasonable purpose (11(1)), and whether in collecting that information Leon's had gone beyond what was "reasonable for meeting the purposes for which the information was collected (11(2)). She found that preventing fraud was a reasonable purpose. She determined, however, that collecting the licence numbers went beyond the statutory limitation set out in section 11(2) of collecting personal information **only** to the extent that was reasonable.

[132] In arriving at that decision, she considered several decisions from the Commissioner's office in which it was held that while it might be reasonable to collect names, addresses and telephone numbers to meet the purpose of preventing fraud, collecting drivers' licence numbers were beyond what was reasonable. One of those cases was the Investigation Report in *Winners*, which she discussed at paras 31-32 of her decision:

> In Investigation Report P2007-IR-006, the Alberta Information and Privacy Commissioner and the Federal Privacy Commissioner were jointly investigating the procedures of a large multinational corporation that was the victim of a security breach in which customers' information was accessed by unauthorized individuals. In their joint investigation the Commissioners commented on the Organization's practice of recording drivers' license numbers, names and addresses when individuals were returning merchandise. It did this in order to discourage fraud and to track customer return habits for indicators of fraudulent activities, such as frequent returns without receipts.

The Commissioners found that although it was acceptable to collect names and addresses of customers returning items, it was not acceptable to record drivers' license numbers. They stated:

> "...a driver's license number is an extremely valuable piece of data to fraudsters and identity thieves intent on creating false identification with valid information. After a drivers' license identity numbers have been compromised, they are difficult or impossible to change. For this reason, retailers and other organizations should ensure that they are not collecting identity information unless it is **necessary** for the transaction." [emphasis in original]

[133] She went on to conclude at paras 34-37 of her decision:

> The statement by [the] Federal Privacy Commissioner and the Alberta Information and Privacy Commissioner in Investigation Report P2007-IR-006 speaks directly to the Organization's argument that it has chosen a safer and less intrusive way of preventing fraud than recording a name, address, or contact information from the person picking up the merchandise as the information it collects is only useful to the police and not to dishonest employees or thieves. Drivers' license numbers are very sensitive pieces of information that are extremely valuable to fraudsters and identity thieves. Several Orders and Investigative Reports published by this Office have made it clear that collecting names and addresses in order to prevent fraud against an Organization is acceptable in some cases but the recording of drivers' license numbers is not.
>
> Therefore the contention by the Organization that its policy of recording of drivers' license numbers is safer and less invasive than collecting names and contact information runs contrary to prior findings of the Federal Privacy Commissioner and the Alberta Information and Privacy Commissioner.
>
> Based on the Investigation Reports and Orders that I have cited, I find that the recording of drivers' license numbers by the Organization is not reasonable for the purposes of the collection and is contrary to section 11(2) of the Act.
>
> I find the same for the recording of license plate numbers of individuals picking up merchandise. In fact, the recording of this personal information has even less reasonable connection to meeting the purposes of the collection than the recording of the driver's licence numbers. As was pointed out by the

> Complainant in her submissions, she could have been driving someone else's vehicle or a rental vehicle. It is unclear to me, how recording that information would assist in the stated purpose of preventing fraudulent pick ups, as there is no way of confirming the identity of the individual at the time of the pick up by looking at the licence plate number of by recording it so as to determine the owner through a registry search.

[134] In my view, there is nothing unreasonable about these findings. Section 11(2) makes clear that an organization can collect personal information "**only to the extent** that is reasonable to meet the purpose for which the information is collected." "Only to the extent" is a limiting provision, and suggests that an adjudicator must examine what personal information is available, and its potential utility, and allow only for the collection of only such information the organization reasonably needs to meet its purposes. Reasonably as defined under section 2 of *PIPA* "...is what a reasonable person would consider appropriate in the circumstances."

[135] In this case, the adjudicator found a breach of section 11(2) on the basis of existing authority holding that the goal of preventing fraud, or catching fraudsters, can be met by collecting other information from the pick up person, such as her name, address and other contact information, that had a less detrimental effect upon her privacy. The principal authority which she applied was the Report of the Federal and Alberta Privacy Commissioners in *Winners*. Due to the adjudicator's reliance on this Report, it is instructive to review the logic that the Commissioners applied in coming to the conclusion that they did.

[136] Winners' difficulties arose when its computer system was hacked into by rogues who made off with, among other things, a bank of drivers' licence numbers. The numbers had been collected and stored to track and prevent fraudulent returns. The Commissioners considered whether the collection and storage of the drivers' licence numbers offended the privacy legislation in their respective jurisdictions. They agreed that identifying and investigating fraudulent returns for loss-prevention purposes was a legitimate activity. They felt, however, that there was nothing unique about a driver's licence number that assisted in identifying a person and his or her shopping return habits. Indeed, all that was required to meet the purpose of loss-prevention was to record "a number– any number – that can be consistently linked to an individual (and one that has more longevity and is more accurate than a name and telephone number)" (para 42).

[137] To the Commissioners, therefore, a driver's licence number was far less useful in identifying fraud artists than the actual name and address on the driver's licence. Balanced against this was the danger, very real in the case before it, that a driver's licence number could be used in identity theft. Thus, they concluded that collecting the name and address on the driver's licence was reasonable for meeting the purpose of loss prevention, but collecting the actual driver's licence number was not.

[138] This logic is spelled out more concretely in *Collection of Driver's Licence Numbers Under Private Sector Privacy Legislation – A Guide for Retailers*, a document distributed by the offices of the Federal, Alberta, and British Columbia Privacy Commissioners. The Privacy Commissioners note at 3:

> Businesses have presented many arguments regarding their purposes for recording driver's licence numbers, or even photocopying the entire driver's licence itself. Some of those reasons are as follows:
>
> to properly identify a person
>
> to deter and detect fraud and other crime
>
> to protect assets
>
> to recover assets, report matters to police or to trace or find someone later
>
> to prove the organization's staff examined identification
>
> to ensure that someone is licenced to drive
>
> By and large, the federal and provincial Privacy Commissioners have agreed with those Canadians who think that recording driver's licence numbers is excessive. The Commissioners understand the organizations' reasons, but they tend to think that they go too far by recording the numbers. **Most of the reasons cited above can be addressed by simply examining identification, recording the person's name as it appears on the licence, or perhaps by also recording the address displayed on the licence**. [emphasis added]

[139] This document also speaks directly to Leon's stated purpose in collecting drivers' licence numbers. Under the heading "Reason: To recover assets, report to police or find someone later" the Commissioners write:

> Many retailers suggest that they can report a person and their driver's licence number to police in the event of a crime (such as fraud), or the driver's licence number can be used to trace a person if property is not returned or there is an outstanding debt. Organizations often think that it will be helpful to police, and easier to find someone, if the driver's licence number can be searched in motor vehicle registries. However, if an organization is already verifying a person's name and address (and perhaps recording the

> information as it appears on the licence), this information in itself will be enough to give to police in almost all cases. Police are able to search motor vehicle registries using a verified name (perhaps cross-referenced with an address) and do not require the driver's licence number.
>
> Similarly, recording a driver's licence number does not necessarily assist the organization itself in finding an individual, since most organizations cannot use this information to access information in motor vehicle registries. Further, the organization has already collected the very information that it would be useful to acquire from such a database – the individual's name and address.

[140] In my view, therefore, there is considerable merit to the logic set out in *Winners* and the adjudicator cannot be faulted for applying it. Leon's purposes in preventing and investigating fraud could have been easily met in this case by requiring that staff ask to see the complainant's driver's licence, and then collecting the name and address on it. This would allow Leon's to ensure that the proper person is picking up the goods, but it would have had a less detrimental effect upon the complainant's privacy than collecting and storing the driver's licence number. The utility of this approach also speaks to the reasonableness of the adjudicator's conclusions about the vehicle licence number. Collecting a number which does not serve to identify the individual picking up the item in question is of limited use in preventing fraud or catching a fraud artist, although it may ultimately reveal personal information about the owner.

[141] I would add, as a postscript, that there was even less need for the personal information here because Leon's already had a great deal of information about the complainant which it could use to track her down in the event of fraud. Along with the personal information it was entitled to collect from her driver's licence, Leon's also had her credit card information, as well as her daughter's address and credit information. It should also be noted that the furniture, in this case, was paid for in full.

[142] It follows that the adjudicator's decision was reasonable as it was transparent, intelligible, and fell "within a range of possible acceptable outcomes which are defensible in respect of the facts and law." Furthermore, the adjudicator relied on authority from the Commissioner's office sanctioning the collection of other personal information to assist in the detection and prevention of fraud that is not as conducive to identity theft, such as an individual's name, address and other identifying information. The Commissioner has developed an expertise in dealing with privacy issues, and assessing the risks that attach to the collection of an individual's personal information. Consistency of approach is important. It follows that a decision of this kind is entitled to considerable deference.

[143] Similarly, I find that the adjudicator's decision with respect to the interpretation and application of section 7(2) was reasonable. The adjudicator held at paras 48-49 of her reasons:

> In my view the key to section 7(2) of the Act is defining what is necessary to provide the product or service. Prior orders have found that the term "necessary" in section 7(2) of the Act does not mean "indispens[a]ble" in the sense that a transaction could not be completed but for the collection of personal information. As the Commissioner stated in Order P2007-016:
>
> > "...if an organization can demonstrate that collection of personal information is necessary to enable it to meet a reasonable purpose relating to a transaction, such as to protect itself against fraud, then the collection may be a necessary condition for the purposes of section 7(2)."
>
> Section 7(2) of the Act must be read in the context of section 11 of the Act (see Order P2006-011 at paragraph 45). As I have found above that the recording of drivers' license numbers and license plate numbers are not reasonably connected to the prevention of fraud under section 11(2) of the Act, I also find that the recording of Complainant's driver's license number and license plate number is not necessary to meet the purpose of prevention of fraud in the purchase and pick up of merchandise.

[144] In essence, the adjudicator found that because she had already found that the collection of the two licence numbers went beyond what was reasonable to achieve the purpose behind Leon's policy, thus amounting to a breach of section 11(2), this finding also established a breach of section 7(2). The test under section 7(2) is whether in requiring an individual's consent the organization has gone "beyond what is necessary to provide the product or service." This section is designed to prevent a form of forced consent. The adjudicator's conclusion that the collection of the numbers was unnecessary to provide the product or service here is clearly reasonable and owed deference.

[145] My colleague suggests it was not unreasonable for Leon's to conclude that collecting the name and address from the driver's licence would be inadequate because "common names are indistinguishable and the address may be out of date" (para 60). But it is difficult to see how these problems would be solved by the use of either licence number. If the police performed a search of the driver's licence number in the appropriate database they would come up with the same name and address that was on the driver's licence. Any other identifying information, such as the height and weight of the licensee, would be just as available by searching the database with the name and address. As far as the vehicle licence number is concerned, that number would only lead to the name and address of the registered owner, information that is no less certain to be accurate than the information on the driver's licence.

[146] Finally, while not necessary to my decision, I note that my colleague, in discussing the application of section 11(2) of *PIPA*, appears to take the position that as long as a policy is reasonably connected to its purpose it would not infringe section 11(2). With respect, I do not agree. The question is not whether information is reasonably connected to the purpose of the policy but whether the information has been collected "**only to the extent"** that is reasonable for meeting the purpose for which the information is collected. This suggests that collection should not go beyond what is actually reasonably required or needed, an interpretation that is consistent with the purpose of the statute. The adjudicator acted quite properly in protecting highly sensitive information, such as the complainant's driver's licence number where its collection was not reasonably necessary.

[147] In summary, the adjudicator did not fail to balance the interests set out in section 3 of *PIPA*. The balancing of those interests takes place, not in any overarching procedure, but in the application of the rest of the statute. In that regard, the adjudicator's decision that Leon's breached sections 11(2) and 7(2) of *PIPA* was reasonable, as the reviewing judge correctly found. The appellant does not dispute the adjudicator's findings with respect to section 13. It follows that this ground of appeal must be dismissed.

E. Issue Four – Did the Commissioner fail to interpret *PIPA* in light of its remedial purpose?

[148] Leon's submits that in interpreting and applying a remedial statute, such as *PIPA*, recourse must be had to the mischief the statute is designed to prevent. Leon's goes on to argue that the statute is designed to prevent identity theft and intrusive marketing activity. Thus, it submits, the adjudicator came to an unreasonable decision by failing to note that Leon's policy does not promote either activity.

[149] I begin by noting that it does not matter whether Leon's policy actively promotes identity theft and intrusive marketing activity. The statute is designed to protect against the opportunity for such abuse by limiting the collection, use and disclosure of personal information. The adjudicator relied on the *Winners* investigation report, P2007-IR-006, in which both the Commissioner, and the Federal Privacy Commissioner, found that the collection of drivers' licence numbers was inappropriate because a driver's licence number "is an extremely valuable piece of data to fraudsters and identity thieves intent on creating false identification with valid information." In coming to this conclusion the Commissioners were not saying that the retailers in question had adopted policies designed to contribute to this kind of fraud. They were saying only that the collection of drivers' licence numbers, where unnecessary, increases the risk that this particularly sensitive information will find its way into the hands of an identity thief. The same is true of Leon's, even if its pick up policy is not designed to promote this kind of activity. Thus, the mischief dealt with by *PIPA* seems to have been very much at the forefront of the adjudicator's analysis.

[150] As the appellant noted in the previous ground of review, the purpose of the statute is set out in section 3. The remedial purpose of *PIPA* is to govern the collection, use or disclosure of personal information in a way the balances an individual's right to privacy with the need of organizations to collect, use or disclose the information for "reasonable" purposes. The adjudicator's reasons indicate that she was alive to this purpose and that it governed her decision.

[151] I conclude, therefore, that the adjudicator did not err in the manner suggested, and the reviewing judge was correct in dismissing this ground of review.

X. Conclusion

[152] For these reasons the appeal must be dismissed.

Appeal heard on September 16, 2010

Reasons filed at Calgary, Alberta
this 28th day of March, 2011

Authorized to sign for: Conrad J.A.

Appearances:

G. Hall and K.L. Smyth
for the Appellant

G.S. Solomon, Q.C.
for the Respondent