OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Order P09-01

CRUZ VENTURES LTD.
(doing business as Wild Coyote Club)

David Loukidelis, Information and Privacy Commissioner

July 21, 2009

Quicklaw Cite: [2009] B.C.I.P.C.D. No. 16
Document URL: http://www.oipc.bc.ca/PIPAOrders/2009/OrderP09-01.pdf

Summary: Section 7(2) of PIPA does not authorize the organization to require customers of its licensed establishment to consent to collection of the scope of personal information that the organization at present collects through use of the driver's licence scanning system in issue here. Nor is it appropriate to collect that scope of personal information in the circumstances.

Statutes Considered: *Personal Information Protection Act*, ss. 7(2), 8, 10(1)(a), 11, 14, 23(1)(b), 34 and 35(2)(b).

Authorities Considered: B.C.: Order P05-01, [2005] B.C.I.P.C.D. No. 18; Order F07-10, [2007] B.C.I.P.C.D. No. 15. **Alta:** Order P2007-016, [2008] A.I.P.C.D. No. 29; Order P2008-004, [2008] A.I.P.C.D. No. 65; Order P2006-011, [2008] A.I.P.C.D. No. 49; Investigation Report No. P2007-IR-006 TJX Companies Inc. (Re), [2007] A.I.P.C.D. No. 34; Order F2005-03, [2005] A.I.P.C.D. No. 23. **Fed:** P.I.P.E.D.A., Settled Case Summary #16; PIPEDA Case Summary #396, [2008] S.C.C.P.V.P.C. No. 9.

Cases Considered: *Re Penny Lane Entertainment Ltd., Penny Lane Entertainment Group, Tantra Night Club Inc*. [2008] A.I.P.C.D. No. 149; Judicial Review application dismissed: *Leon's Furniture Limited v. Sharon Curtis, The Information & Privacy Commissioner, et al* (18 June 2009), Calgary No. 0801-12471 (Alberta Q.B.); *Penny Lane Entertainment Group v. Alberta (Information and Privacy Commissioner)*, [2009] A.J. No. 300; 2009 ABQB 140; *Re Home Depot of Canada,* [2008] A.I.P.C.D. No. 29; *Wood v. Commissioner of Police for the Metropolis* [2009] EWCA Civ 414.

TABLE OF CONTENTS

1.0 INTRODUCTION

[1] This decision deals with a complaint from someone who visited Vancouver's Wild Coyote Club ("Wild Coyote"), an establishment licensed to serve liquor. At the door, Wild Coyote employees asked the complainant to produce his driver's licence. They then swiped the licence through a card reader and required the complainant to have his digital photograph taken. The complainant did not receive what he considered to be a reasonable explanation as to why his personal information was being collected and later complained to this Office.

[2] Because the matter was not resolved in mediation, it was referred to an inquiry under s. 50 of the *Personal Information Protection Act* ("PIPA"). Submissions were received, but I determined there was not sufficient evidence and argument to enable me to properly consider the merits and make a decision. Accordingly, I referred the matter for further investigation by this Office.

[3] The further investigation led to the November 5, 2007 'Investigation Report on Wild Coyote Club (Cruz Ventures Ltd.) and its Use of Identification Scanning Software from TreoScope Technologies' ("Investigation Report").[1]

[1] A copy of the Investigation Report is appended to this decision.

I then reconvened the inquiry under PIPA for the purpose of making findings and an order under PIPA on the merits of the complaint.

[4] I received submissions from the complainant and Wild Coyote. I also asked for and received submissions from the following: BC Civil Liberties Association ("BCCLA"), TreoScope Technologies Inc. ("TreoScope"), Barwatch, Alliance of Beverage Licensees ("ABLE BC"), BC Association of Municipal Chiefs of Police ("The Chiefs' Association"), BC Liquor Control and Licensing Branch ("Liquor Branch") and the Insurance Corporation of British Columbia ("ICBC").

2.0 ISSUES

[5] The Amended Notice of Written Inquiry that this Office issued sets out the following issues to be determined at this inquiry:

1. Is the complainant deemed to have consented to the collection, use and disclosure of the information in compliance with s. 8 of PIPA?

2. Did the organization, Wild Coyote, disclose the purposes for the collection of the personal information to the complainant verbally or in writing as required by s. 10(1) (a) of PIPA?

3. Did Wild Coyote's collection of personal information meet the requirements of s. 11 of PIPA?

4. Did Wild Coyote's use of the personal information meet the requirements of s. 14 of PIPA?

5. Did Wild Coyote provide the complainant with information about the ways in which the personal information has been and is being used as required by s. 23(1)(b) of PIPA?

6. Has Wild Coyote made reasonable security arrangements to protect the personal information as required by s. 34 of PIPA?

7. Is Wild Coyote retaining the personal information no longer than is necessary for legal or business purposes, in accordance with s. 35(2)(b) of PIPA?

[6] In the original Notice of Written Inquiry, the question of whether Wild Coyote's collection, use and disclosure of information complies with s. 7 of PIPA was identified as one of the issues. The Portfolio Officer's Fact Report also said that the complainant had identified compliance with s. 7 as an issue. Section 7 was not, however, identified as an issue in the Amended Notice of Inquiry, which

was issued after the Investigation Report was complete. Section 7(2) was, however, addressed in the submissions of TreoScope and the BCCLA.[2]

[7] In order to ensure that all participants had a fair opportunity to comment on the application of s. 7(2), I invited further submissions on that issue and received submissions from Wild Coyote, TreoScope, ABLE BC, the Chiefs' Association, the Liquor Branch and Barwatch. The BCCLA did not provide any new submissions on s. 7(2), but it did reply to the further submissions of the others. TreoScope objected to this, on the basis that the BCCLA had not provided "initial submissions" in response to my invitation for submissions on s. 7(2). Each of the participants was then provided with a further opportunity to reply to the BCCLA's submissions and the BCCLA was given an opportunity to reply to those, but none of the parties or interveners provided further submissions.

3. DISCUSSION

[8] **3.1 Background**—The following facts are taken largely from the Investigation Report, which was provided to the parties for comment.

[9] When the complainant tried to get into Wild Coyote, employees asked for his driver's licence, swiped the licence through a card reader and required him to have his photograph taken by a surveillance camera before he would be allowed to enter the club. The complainant observed that this requirement was being applied to every customer who entered the club. He asked if he could "refuse consent" and was told that the scanning was required to get into Wild Coyote. Before he was given the opportunity to refuse to have his licence scanned, the door staff had already scanned it, thus collecting his personal information. Seeing that his personal information had already been collected, he entered Wild Coyote. When he left, the complainant spoke with a man, whom he identified as a supervisor, and asked what the purpose of the scanner was. The complainant says he was then told that his personal information would only be held and accessed by a third-party business that provided the ID scanning system to Wild Coyote.

[10] The scanning system used by Wild Coyote is the Vigilance Software system, a security product developed and maintained by TreoScope. Wild Coyote employs the system under a contract with TreoScope. Wild Coyote depends on TreoScope for technical support and retrieval of personal information.

[11] As indicated in the Investigation Report, when a customer enters the main door of Wild Coyote, he or she is led into a small anteroom in which door staff

[2] In addition, many of the earlier submissions specifically addressed the issue of whether the collection of information by the TreoScope software is "necessary" and so these are relevant in considering the s. 7(2) issue.

ask for identification ("ID") (usually a driver's licence or a BC ID, a government identification card issued to non-drivers on their request). A Wild Coyote staff member then swipes the ID card through a reader not unlike those used in stores to swipe debit or credit cards. When the card is scanned, the system records information that is found on the card's magnetic strip. The system collects the following personal information from the card: driver's licence number, name, sex, date of birth and partial postal code.[3]

[12] The partial postal code that is gleaned from a customer's ID is not stored in a way that is connected to the customer's profile; it is used for demographic statistics only. For example, the partial postal codes could be extracted from the system by TreoScope and used to indicate the general areas in which customers live, so that Wild Coyote could better target its advertising efforts.

[13] On the right-hand side of the anteroom there is a small computer (which is where the information from the magnetic strip on the ID is stored) and a computer screen (which displays the customer's information after her or his ID is scanned). A small camera embedded in the wall a few feet above the computer screen takes the customer's photograph. This photograph is matched to the information scanned from the ID and is also stored on the computer. After the ID has been scanned, the customer is allowed to proceed through another set of doors and then enter Wild Coyote itself.

[14] The system also records the date and the time that the customer entered the premises and tracks the number of visits by each customer to Wild Coyote ("Familiarity Index"). Wild Coyote is able to create notes in the system about customers whose involvement in an incident, in Wild Coyote's view, warrants this action. For example, if a customer becomes violent and is removed, notes about the incident can be recorded in the customer's system profile. Conversely, if Wild Coyote wishes to label a customer as a VIP, the system allows that to be done. The notes can vary in descriptiveness and may range from a few words such as "evicted for fighting" to several paragraphs, depending on the nature and severity of the incident.[4] Essentially, a profile is kept of each customer of Wild Coyote.

[15] In August 2007, TreoScope introduced a version 2.0 of its Vigilance Software, called EnterSafe Gateway Security. The same data elements continue to be collected by the software but less information is visible to users at Wild

[3] As explained in the submissions received from ICBC, driver's licences and BC ID cards have two encoded sections: a magnetic stripe and a 2-d bar code. These areas contain the licence number, physically identifying information, the class of licence, any restrictions on driving and the individual's name and residential address. The encoded areas do not include the photograph or signature. As a result, the collection of the photograph by Wild Coyote is through the digital photograph taken at the time of entry, while the other information is extracted from the encoded sections of the ID.

[4] At the time of the investigation, there was no written policy on what should or should not be included in notes about customers.

Coyote. Only a customer's name, calculated age and digital photograph are visible to Wild Coyote. Before, a customer's date of birth, driver's licence number and sex were visible.

[16] Changes have also been made to the length of time scanned information and notes typed into the system can be viewed by Wild Coyote. Under the new system, if a customer enters Wild Coyote and there is no recorded "incident", and the customer does not visit again within the next six months, all of that customer's personal information becomes inaccessible to Wild Coyote. The information remains on the system in such cases, but it can only be retrieved by TreoScope.[5] If a customer comes back within six months, the clock resets and the customer's name, calculated age and digital photograph are visible to Wild Coyote for another six months.

[17] If a customer is involved in an "incident" at Wild Coyote, Wild Coyote may write an internal report about that customer which may be visible to Wild Coyote employees, at the discretion of Wild Coyote's owner, from a minimum of seven days to a maximum of one year.[6] If there are no further incidents within the one-year period, that information becomes inaccessible to Wild Coyote, but is still stored for two years on the database. If a second internal report is written within the one year, the original report is visible until the expiry date of the second report. Further, if that second report is written about a person after one year but before the two-year anniversary date, the first report will be visible to Wild Coyote until the expiry date of the second report or until the two-year anniversary date, whichever comes first. All report information about a customer is deleted from the database two years from its creation.

[18] These same conditions apply to 'alerts', which can be entered into the system if the business wants other establishments to have access to the information. Wild Coyote does not at this time share information through the system with any other businesses and it is not connected to the internet. If Wild Coyote decided to implement the information-sharing option, other establishments would be able to see information about a Wild Coyote customer if there were incident notes about that customer at Wild Coyote and that same individual's ID was scanned at another business that uses the same TreoScope system.

[19] TreoScope, in an attempt to help maintain the integrity of notes entered into the system about customers, has added a 'disclaimer' screen that requires the system user to "accept" or "decline" responsibility for the information they

[5] I will note here in passing, without deciding the matter, that TreoScope's authority to hold personal information of the customers of an organization for which TreoScope provides services, such as Wild Coyote, depends on the service relationship between TreoScope and the customer organization. Section 12(2) of PIPA addresses this.

[6] TreoScope said it is developing a severity level index that will assist businesses in determining what types of incidents warrant different severity ratings, but the index was not yet complete at the time of the inquiry.

record and the accuracy of that information. TreoScope has also added an advanced audit trail that allows it to track all access movements by a user in the user interface should an allegation of misuse need to be investigated.

[20] The software includes various access levels. Most employees at Wild Coyote can only view customer profiles of customers who are in the club on any particular night. Wild Coyote managers have access levels that authorize them to view the profiles of customers, regardless of whether or not the customers are in the club on a particular night, and to write notes on any customer's profile. Wild Coyote has said it only allows "necessary employee access"[7] to the system. For example, wait staff would not have access, but door staff would.

[21] The software has multiple layers of access control that ensure Wild Coyote has no access to the raw data or the software itself. The software also does not allow Wild Coyote to print, copy or in any way extract information from the database without the assistance of TreoScope.

[22] The Investigation Report says the "software" is protected with 256-bit encryption.[8] TreoScope says that, even if the encryption is broken, further security lies in the fact that the information is stored in separate and unidentifiable tables that cannot be reconciled without a specific key (or map) that is stored offsite.

[23] **3.2 Mandatory Consent?**—As noted earlier, while s. 7(2) of PIPA was not set out as an issue in the Amended Notice of Inquiry, it was identified as an issue by the complainant and all parties have had a full opportunity to address it.

[24] Section 7(2) of PIPA limits an organization's ability to collect personal information as a condition of supplying a product or service:

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

[25] Wild Coyote's supplemental submission says "the TreoScope system is a tool my establishment has deemed necessary to restrict the entrance of minors and to ensure that customers and staff are safe." Wild Coyote notes that, in previous submissions, many interveners supported the position that collection of personal information through the TreoScope system is "necessary". The Chiefs' Association asserts that "the collection, use and disclosure of personal information facilitated by the TreoScope system is demonstrably necessary to

[7] Investigation Report, para. 39.
[8] Investigation Report, para. 41.

provide for a safe and secure environment for [Wild Coyote's] patrons and staff." Wild Coyote notes that Barwatch, an association of licensed establishments discussed below, takes the position that the use of the TreoScope software is necessary by making it mandatory for its members. As well, Wild Coyote notes that the Liquor Branch has, in some instances, ordered establishments to use scanning technology as a condition of their licence. In its supplementary submission, ABLE BC says that "the supply and recording of identification is necessary to provide our service and to protect our customers and the public." In their supplemental submissions, many of the interveners restate their position that the use of the software is "necessary".

[26] However, Wild Coyote also says that all customers can choose to surrender their physical ID for the duration of their visit to the club as an alternative to having their ID scanned and that as a result customers are not required to have their ID scanned as a condition of entry. The evidence about whether Wild Coyote's customers are offered an alternative to having their IDs scanned has been contradictory. The complainant was told that he would not be admitted to the Wild Coyote unless his ID was scanned. In its first submission, Wild Coyote said this

> Should a customer have a legitimate reason for not wishing to have their identification scanned our internal policy is to have a manager…or myself contacted. At this time, we offer the customer alternative solutions such as; [*sic*] leaving ID with us until the end of the night. We have had two customers ask for this in the past few years and neither has complained about the alternative solution provided.

[27] As part of this Office's investigation, a Portfolio Officer visited Wild Coyote to test this policy. The Portfolio Officer tried to enter Wild Coyote (without identifying himself as an OIPC employee in doing so). He was asked at the entrance for his ID so that it could be scanned into the system. The Portfolio Officer said he did not want his ID to be scanned, but still wanted to enter the premises. He was told that he would not be allowed in unless he allowed his ID to be scanned. The Portfolio Officer was not permitted to speak to the manager.[9]

[28] The following day, the Portfolio Officer interviewed Wild Coyote's manager ("Manager"). The Manager said that if a customer does not want to have her or his ID scanned, the Manager will hold the ID until the customer leaves. When he was told what had happened the night before, the Manager said he would take immediate steps to correct the practice and to provide the employee in question with appropriate training on properly handling driver's licences, as required by this Wild Coyote policy.[10] In its supplemental submissions on s. 7(2), Wild

[9] Investigation Report, para. 18.
[10] Investigation Report, para. 19.

Coyote says it "adopted the practice of allowing an alternative method of entry after being advised to do so in a meeting with OIPC investigative staff."[11]

[29] In any case, Wild Coyote now takes the position that customers may refuse to have their ID scanned if they agree to leave their ID with management until the customer leaves. Wild Coyote says that, while its practice had been to retain a customer's ID in the manager's pocket, TreoScope told it "to take the same measures of security around a physical ID as the software takes."[12] As a result, Wild Coyote now keeps IDs in the office safe. It says that, "in close to five years, our establishment has only been asked five or so times for an alternative form of entry."[13]

[30] Wild Coyote argues that, because it offers this alternative, consent to the collection of information through the TreoScope system is not a condition of entry to Wild Coyote. As the BCCLA points out, however, collection by way of retaining the physical ID is still a collection and Wild Coyote has not said that customers are given the option of refusing consent to collection of their personal information in this other way.

[31] The Liquor Branch's supplemental submission on s. 7(2) says this:

> I noted at paragraph 14 of my previous letter that where use of scanners and video technology is reasonably necessary to prevent minors from accessing liquor and to promote the safe operation of the establishment that it must apply to every patron. From the perspective of the management and control of licensed establishments, leaving identification at the door while a patron will generally be a suitable alternative to scanning and video recording. … However, in the exceptional circumstances where the use of scanning technology is imposed as a term and condition of the liquor licence in order to promote public safety permitting customers the option of not having their identification scanned, even if it was left at the door, would not be acceptable.[14]

[32] No one suggests that use of a scanner has been imposed as term of Wild Coyote's licence. Both Wild Coyote and the Liquor Branch appear to agree, therefore, that an acceptable alternative is to hold a customer's ID while the customer is at Wild Coyote.

[33] It is clear that it is a condition of entry that customers must either surrender their IDs or consent to having them scanned. The question then is, does this require patrons to consent to the collection, use or disclosure of personal information "beyond what is necessary to provide the product or service"?

---

[11] Wild Coyote Supplemental Submissions, December 16, 2008, para. 16.
[12] Wild Coyote Supplemental Submissions, December 16, 2008, paras. 24-25.
[13] Wild Coyote Supplemental Submissions, December 16, 2008, para. 22.
[14] Liquor Control and Licensing Branch, Supplemental Submissions, December 17, 2008, pp. 1-2.

Are the collection and use of the information "necessary"?

[34] Wild Coyote and several of the interveners rely on my finding, in Order P05-01[15] ("*Gostlin*"), that the word "necessary" in s. 7(2) of PIPA does not mean "indispensable". In *Gostlin*, I considered the meaning of the word "necessary" as it applied to the collection of a customer's name, address and telephone number as a condition of accepting merchandise for return. The organization, a retailer, provided evidence which demonstrated that it faced ongoing challenges from successful fraudulent returns of goods, with the company suffering losses each year as a result. I held that the overall statutory context and the language of s. 7(2) suggested that the Legislature did not intend to create a strict standard of indispensability by using the word "necessary", saying this:

> [78] Personal information may be "necessary" under s. 7(2) even if it is not indispensable. Of course, personal information may, in some cases, be "necessary" in the sense that is not possible to supply a product or service without the personal information or because it is legally required for the supply. But there will be cases where personal information is necessary even though it is not, when considered in a searching yet reasonable manner, indispensable in the sense that is not possible to supply the product or service without the personal information.

[35] In *Gostlin*, I considered the nature of the information collected, the purpose of the collection, and the scope of the collection in determining that the collection of the information was necessary for the purpose of providing the service of accepting returns for a refund. In that case, the organization also used the information it collected for the purpose of customer satisfaction follow-up and I found that collection and use of the information for that purpose was not necessary for the supply of the product or service in question. There was also some evidence in *Gostlin* that the organization in some cases asked for photo identification to confirm identity, prompting me to say this:

> [97] Although a preliminary view, and the circumstances of each case would govern, I have some doubt that an organization is able to compulsorily collect or use personal information from identification such as a driver's licence on the basis that the information is "necessary" within the meaning of s. 7(2). I would think it is enough for the organization to examine the identification, which is what the organization does in this case, and then record the fact that it was produced and examined to the organization's satisfaction.

[36] Other PIPEDA decisions have taken a similar approach, as have decisions of the Office of the Information and Privacy Commissioner of Alberta under Alberta's *Personal Information Protection Act* ("Alberta PIPA"), which is

[15] [2005] B.C.I.P.C.D. No. 18.

similar to our PIPA. In Order P2007-016,[16] Commissioner Frank Work interpreted the word "necessary" in s. 7(2) of Alberta PIPA, the language of which is for all intents and purposes the same as our s. 7(2). His interpretation of "necessary" is the same as that in Order P05-01.

[37] A 2007 case required me to interpret the term "necessary" in the context of the public sector privacy provisions of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). In Order F07-10,[17] I noted that, while the purpose of FIPPA is to protect personal privacy, the overall statutory context is one which recognizes that public bodies must collect personal information in order to do their work. I held as follows:

> [48] The collection of personal information by state actors covered by FIPPA—including local public bodies such as the [school] Board—will be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of FIPPA. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.

[38] I went on to say that, even in the FIPPA context, it would not be necessary for the information to be indispensable, and that the factors to be considered in determining necessity include the sensitivity of the information, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purposes for collection.

[39] As I noted in *Gostlin*, PIPA recognizes, as s. 2 says, "both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." While FIPPA's purpose provision does not explicitly contemplate this same balancing of competing interests, the interpretation of the term "necessary" in FIPPA occurs in light of the fact that the context of FIPPA requires recognition of both the legitimate governmental interest in collection of personal information and the public interest of privacy protection. As a result, there is likely to be a substantially similar meaning to the term "necessary" in the two statutes.

[40] While organizations may not be held to the same rigorous standard of necessity as public bodies under FIPPA—which after all do not in most instances under FIPPA need consent to collect citizens' personal information—personal information must certainly be more than simply convenient to have or of some possible future use. For personal information to be "necessary" for the purposes of s. 7(2) of PIPA, the purposes for the collection, use or disclosure must be integral to the provision of the product or service. In addition, the personal

[16] [2008] A.I.P.C.D. No. 29.
[17] [2007] B.C.I.P.C.D. No. 15.

information in question must fulfill a significant role in enabling the organization to achieve that purpose. It is also important for the organization's purposes to be stated as precisely as possible, avoiding overly generalized objectives. In addition, it is necessary to consider whether the scope of the collection is appropriately tailored to the purposes for which it is collected. In assessing these questions, the sensitivity of the information may play some role in determining the level of scrutiny to be applied.

[41] It is also appropriate to consider whether there are less privacy-intrusive means of achieving a legitimate purpose. In Alberta Order P2007-016, the Commissioner held that it was not "necessary" within the meaning of s. 7(2) for a retailer to record driver's licence numbers as a condition of accepting goods for return. As already noted, the Commissioner interpreted "necessary" in the same way as I did in Oder P05-01. In finding that necessity had not been established, he made the following finding:

> The Organization states that its return policy authorized employees to provide a full return without recording driver's license numbers if the customer produced a receipt and the price of the items was confirmed. Because it had a policy in place to enable it to meet its purpose of reducing the potential for fraud without collecting driver's license information, I find that it was unnecessary for the Organization to require the Complainant's driver's license before providing a full refund.[18]

[42] In this case, as in *Gostlin*, the organization asserts that a purpose of the collection is to detect and deter illegal activity by customers. This raises the prospect of private organizations forcing their customers to provide personal information so that the organization can freely disclose it to the state if illegal activity of some kind occurs. On the other hand, if there is evidence of ongoing illegal activity which has a negative impact on an organization's ability to provide a product or service, the detection and deterrence of the illegality may be found to be integral to the provision of that service. The question then becomes whether the collection, use or disclosure of the personal information significantly assists in achieving the organization's purpose by detecting and deterring the activity.

---

[18] At para. 21. Also see Alberta Order P2008-004, [2008] A.I.P.C.D. No. 65. In that case, it was held that collection of a driver's licence number and vehicle licence plate number was not "necessary" for the purpose of picking up purchased furniture (para. 49). This order has been upheld on judicial review: *Leon's Furniture Limited v. Sharon Curtis, The Information & Privacy Commissioner, et al* (18 June 2009), Calgary No. 0801-12471. The joint investigation report of the Alberta Commissioner and the Privacy Commissioner of Canada, published by the Alberta Commissioner as Investigation Report P2007-IR-006, TJX Companies Inc. (Re), [2007] A.I.P.C.D. No. 34, arrived at a similar conclusion, at para. 46. Last, I note that Commissioner Work has held, under Alberta's *Freedom of Information and Protection of Privacy Act*, that a collection of personal information is necessary "only when there is no less intrusive way of collecting sufficient information to address a particular management issue". Alberta Order F2005-03, [2005] A.I.P.C.D. No. 23, at para. 30.

[43] I will note here that PIPA does not explicitly address where the burden of proof lies in relation to s. 7(2) compliance. The general framework of PIPA is to require consent to be voluntarily given to any collection, use or disclosure of information, subject only to certain exceptions. Despite being cast in the negative, s. 7(2) authorizes organizations to require consent to collection, use or disclosure of information as a condition of supplying a product or service only to the extent that it is necessary to provide the product or service. Accordingly, it is appropriate that the organization bear the burden of demonstrating that what it is doing complies with s. 7(2). My conclusion is reinforced by the fact that generally the organization is the party that is in a position to demonstrate that the collection, use or disclosure is necessary in order for it to provide its product or service.

[44] It is necessary to examine the purposes for which Wild Coyote collects the personal information in question in order to determine whether the collection is necessary for the purpose of providing the service of operating a licensed establishment. According to the Investigation Report, Wild Coyote says it collects personal information of customers for the following purposes:

1. To provide a safer environment for customers;

2. To prevent minors from entering the premises;

3. To keep a record of customers who have been banned from Wild Coyote;

4. To keep a record of customers in case the information is needed for a court action involving Wild Coyote or in case it is required by law enforcement to investigate a crime.

Preventing minors from entering

[45] Wild Coyote says one of the purposes of using the TreoScope system is to prevent minors from entering the club. Section 33(1) of the *Liquor Control and Licensing Act* ("Liquor Act") says that a "person must not sell, give or otherwise supply liquor to a minor", *i.e.*, someone under 19 years of age. Section 33(5) of the Liquor Act says the following:

> (5) It is a defense to a charge under this section if the defendant satisfies the court that, in reaching the conclusion that the person was not a minor, the defendant
>
> (a) required that the person produce identification, and
>
> (b) examined and acted on the authenticity of the identification.[19]

[19] I note here, in passing, that this provision says nothing about the methods a licensee must or may use to examine and act on the authenticity of identification offered by a minor.

[46] Section 45(1) of the Liquor Control and Licensing Regulation ("Liquor Regulation"),[20] made under the Liquor Act, provides that identification must consist of two pieces of identification, one of which must be a passport, a driver's licence or a government-issued identification card displaying a photograph and the date of birth of the holder. TreoScope submits that, as a practical matter, this means that bars and nightclubs must ask customers to show their driver's licence on entry.[21]

[47] TreoScope also notes that the terms and conditions of the liquor licence issued to bars and nightclubs set out suggested procedures, and potential directives of the liquor inspector for bars and nightclubs, for proper maintenance of their liquor licences:

> If you operate an establishment that is particularly attractive to young people, you will be expected to maintain a sufficient standard of scrutiny to prevent access to minors. To help deter minors, we suggest you:
>
> - Record each person's name and the ID serial number
> - Assign an experienced doorperson to check ID
> - Secure any uncontrolled exits, as allowed in fire safety rules, regulations or codes, and
> - Use video surveillance to record an image of the person and his or her ID.
>
> If your procedures are not effective, your local liquor inspector may direct you to install the appropriate lighting, signage, video cameras and noise barriers to ensure your staff can check identification properly. (Licensees directed to install and operate video cameras may be required to provide the file from those cameras for review by the branch.)[22]

[48] Wild Coyote believes that the TreoScope system assists with preventing minors from entering its premises. This is because of the system's ability to detect fake ID and to prevent minors from "ID passing".[23] If the card presented at the door is not properly encoded, as it would be if it were a valid driver's licence or BC ID, the machine will not be able to read it, thus alerting door staff. Any such card that was originally valid but has been visually altered will record and display the original information on the magnetic strip, alerting the door staff when information on the card does not match information displayed on the computer screen.[24] As for ID passing, if someone's card is used more than once

---

[20] B.C. Reg. 244/2002.
[21] TreoScope second submission, para. 26.
[22] TreoScope second submission, para. 27; Investigation Report, Appendix 5.
[23] "ID passing" happens when a customer who has entered with his or her legitimate ID passes it to another person outside, who then tries to use the ID to get into the premises.
[24] Investigation Report, para. 23.

on the same day, the photograph from the first entry is displayed and door staff can compare that photo to the person standing in front of them.[25]

[49] In its initial submissions, made before the Investigation Report, Wild Coyote said it had "dropped underage passing of ID's (multiple use of the same ID in one night, allowing a minor to gain access) by nearly 99%" as a result of the TreoScope technology.[26] The Investigation Report said this, however:

> [27] During the interview with Mr. Bell [the Manager of Wild Coyote] on April 20, 2007, he admitted that the WCC has not had a substantial problem with infractions under the *Liquor Control and Licensing Act* (LCLA) and could not conclusively state whether the system has had an impact on minors unknowingly [*sic*] entering the WCC. He stated that, based on his experience, the average age of the customers at the WCC is 19 to 24 years of age so the possibility of minors attempting to access the premises was always a concern. An online search of the Liquor Control and Licensing Branch's enforcement decisions reveals that the WCC has only been involved in two enforcement actions which occurred on December 17, 2003 and June 8, 2004. The two infractions were regarding overcrowding and not having the appropriate red-lined floor plan available for inspection as required by the LCLA. The WCC was also issued a Contravention Notice on March 1, 2003, for having minors on the premises, but no enforcement action was taken.
>
> [28] The WCC believes the system provides important evidence in making a due diligence defence if enforcement action, regarding minors, is taken against them. For example, with information from the system, Wild Coyote will be able to show police and/or Liquor Control Inspectors photographs of every customer they admitted to the bar and proof that their ID was checked. This proof, they believe, will prevent minors from entering the premises therefore preventing possible fines or suspension of their liquor licence.

[50] Wild Coyote's second submission, made after the Investigation Report, notes only that there have been instances where passed or fraudulent ID has not been caught by the first visual screening by an employee but was identified by the TreoScope software.[27]

[51] As part of this Office's investigation, an audit was performed of Wild Coyote's incident reports for several months before and after its adoption of the TreoScope system. As regards this audit, the Investigation Report noted that, after the system was put into use, an incident occurred where a customer, who did not have ID, was found in the club by police and was later noted to be well known to Wild Coyote employees and thought to be of age.

---

[25] Investigation Report, para. 24.
[26] Wild Coyote initial submission, p. 2.
[27] Wild Coyote second submission, p. 6.

[52] TreoScope's initial submissions claim that its product has resulted in a "90% reduction in minors gaining access" to establishments using the system.[28] TreoScope's second submission, in contrast, sets out the legislative regime that requires bar owners to ask customers to produce identification in order to ensure they are of legal drinking age.[29] The submission goes on to note that establishments that do not use its system must rely on visual inspections of driver's licences, which TreoScope asserts cannot detect fraudulent ID as effectively as its technology.[30] TreoScope's submission includes two customer testimonials, one of which relates to an establishment that was able to establish a due-diligence defense when a minor was found to be drinking in the establishment.[31]

[53] The Barwatch submission says this

> Members of Barwatch have repeatedly mentioned how the software has caught ID's that were fraudulent or passed that their security personnel had missed.…Further, we have had a number of members who have satisfied their due diligence defense through the use of TreoScope's software often without ever having to go to a hearing.[32]

[54] The BCCLA argues that, even if it is necessary to scan the IDs of younger customers, there is no need to scan the IDs of customers who are clearly of drinking age. In addition, the BCCLA says no benefit is gained by recording the ID information, rather than just having it checked by door staff. Further, and in the alternative, the BCCLA says that, if it is necessary to record the information to prevent ID passing, it could be erased the next day with no adverse consequences.[33] In response, the Liquor Branch asserts that police and liquor inspectors may conduct covert operations and licensees may not be aware of this activity, or a proposed sanction, until as many as three weeks after a covert operation. It says that "99% of all enforcement actions have been finalized within 9 months of a contravention."[34] I note, however, that the Liquor Branch also says it has, in at least one instance, required an establishment with a history of gang violence and permitting minors to enter to use ID scanning technology:

> In another situation a licensee with a history of gang activity and permitting minors had a term and condition added to their licence to install, use, and maintain both an electronic weapons detection system and electronic ID scanning equipment. The establishment was required to retain one week's worth of data that could be made available to the police and liquor inspectors.[35]

---

[28] TreoScope initial submission, para.1.
[29] TreoScope second submission, paras. 24-27.
[30] TreoScope second submission, para. 44.
[31] Affidavit Owen Cameron, Exhibit "E".
[32] Barwatch second submission, p. 4.
[33] BCCLA second submission, paras. 36 and 37.
[34] BC Liquor Control and Licensing Branch submission, paras. 18-19.
[35] BC Liquor Control and Licensing Brach submission, para. 13.

[55] Given the regulatory framework, the collection of some identifying information to verify some customers' age is an example of a collection which is "legally required", as I used that term in *Gostlin*. As noted above, a licensed establishment is required to take some steps to prevent underage customers from entering. The question remains, however, whether the collection and recording of *all* customers' personal information in a computer database is "necessary".

[56] First, I agree with the BCCLA that it cannot be "necessary" to scan the IDs of those patrons who are clearly over legal drinking age. Even as regards those who may not be of age, there is no evidence that the entry of minors was a significant problem for Wild Coyote. In *Gostlin*, the organization collected personal information to detect and deter fraudulent returns of stolen goods. The organization processed 200 returns on an average day, for a total of approximately 70,000 return transactions per year. The evidence there established that the organization incurred "material and significant" losses from fraudulent returns. I found that the evidence had established there to be a "real, not perceived or minimal, problem with return of stolen goods." By contrast, the evidence here does not establish that attempted entry by minors is or was a prevalent, significant problem at Wild Coyote.

[57] Nor am I persuaded that use of the TreoScope system significantly assists Wild Coyote with achieving the purpose of preventing the entry of minors. Both the incident report created after Wild Coyote adopted the software—the report which showed a minor had been on the premises—and the content of the above-cited TreoScope testimonial, suggest that the system is perhaps not as effective in addressing the actual problem of underage entry as it might be in enabling Wild Coyote and other establishments to establish a due diligence defence. It is not apparent why Wild Coyote cannot establish a due diligence defence if it ensures that its staff without fail check IDs visually where appropriate.

[58] Finally, there are less privacy-intrusive means of achieving the organization's purpose. ID scanning has been the subject of a complaint under PIPEDA. A Manitoba bar had collected an individual's personal information using an ID scanner without her knowledge or consent. When the information was collected, there was no sign in place which notified would-be customers of the information collection. While this was enough to uphold the individual's complaint, Assistant Commissioner Elizabeth Denham also considered whether the purposes for the collection were reasonable. She rejected the organization's contention that the system "verified age", noting that the employee who scans the ID, and not the machine, compares a customer's face to the photograph on the ID and checks the birth date. The Assistant Commissioner noted that "[a]n equally effective and far less privacy-invasive means of ensuring age

compliance is to have staff look at the identification and verify the age and identity of individuals entering the premises."[36]

[59] In the absence of any real evidence going to the prevalence of ID passing and the effectiveness of the software, as opposed to the traditional method of checking IDs visually, in ensuring that minors are actually prevented from entering the bar, I find that collection of the personal information through the TreoScope software for this purpose is not "necessary".

[60] The same concerns apply to the alternative practice of holding the IDs while the patron is in the establishment. It is not necessary, for the purposes of preventing the entry of minors, to collect the IDs of those who are clearly overage. With respect to those who are not clearly of age, door staff can check the authenticity of the ID at the time of entry—it is not necessary to retain the ID. While holding the IDs would seem to address the problem of "ID passing", there is no evidence that this was or is a significant problem at Wild Coyote. In this regard, it is important to note that the government regulations require one of the pieces of ID to be checked to be ID with a photograph, so that door staff will always be checking to see whether the patron before them matches a photograph, whether that photo is on the TreoScope system or on the ID itself.

Defending liability claims and helping police investigations

[61] As the Investigation Report indicates, Wild Coyote has said that one of the purposes for the collection is to keep a record of customers in case the information is needed for a court action involving Wild Coyote or in case it is required by law enforcement to investigate a crime.

[62] No doubt all kinds of businesses might find themselves in a better position to defend liability claims if they had a record of everything that occurred on their premises and information to tie specific customers to incidents. There is, however, no evidence that Wild Coyote or any other establishment has ever used the information stored in the TreoScope system to defend a liability claim of any kind.

[63] As for possible investigative use by law enforcement agencies, there is evidence that in three cases police sought access to Wild Coyote's records during investigations. But there is nothing to suggest that, apart from the fact that they involved someone who was a customer of Wild Coyote at one time, the incidents which led to the investigations were otherwise connected to Wild Coyote.

[64] In these circumstances, I find that the stated purpose for which the collection is made is not directly related to the provision of the service of

[36] PIPEDA Case Summary #396, [2008] S.C.C.P.V.P.C. No. 9.

operating a nightlife establishment and therefore cannot assist the Wild Coyote in establishing that such collection is necessary for the purposes of s. 7(2).

Providing a safe environment for customers

[65] Wild Coyote's submissions assert that the use of the TreoScope system "has hugely advanced [its] security and safety procedures." Wild Coyote asserts it is "faced on a daily basis with violence towards customers and staff, drug trafficking, drink tampering (doping), sexual assault, property damage, underage drinking, and gang activity". It says the software "has been the best tool we have deployed and has resulted in the greatest reduction of these issues."[37] As noted earlier, Wild Coyote's initial submission says use of the TreoScope system "decreased the number of fights by 80%".[38]

[66] Yet Wild Coyote could not demonstrate, in support of these assertions, a decrease in the number of incidents at the premises as a result of the use of the system. As noted, this Office's investigation included a review of Wild Coyote's records of incidents in the establishment, and the resulting Investigation Report says this:

> [43] The Wild Coyote Club ("WCC") has for many years kept a hand written logbook of any incidents that take place on their property on the days the business is open. The incident log keeps record of which employees were on shift that night, whether or not there were any incidents and details of each incident. It may also include notes on how busy the bar was and whether the police visited the premises. During the site visit we asked to see the handwritten incident log covering the period of the complaint but that log book was not immediately accessible. Mr. Bell agreed to provide select photocopies from the incident logbook of the twelve consecutive months of records beginning six months prior to the installation of the Vigilance software to 6 months after the installation. Records received from Wild Coyote included only dates from January 31st 2004 until December 23rd, 2004 so only records from February 10 until November 10 were used for the audit (*i.e.* a total of ten months of records). The exact date of the Vigilance software installation is unknown. The complainant says the system was in place on June 12, 2004 and WCC states that it installed the system sometime in June 2004.
>
> [44] The intent of the audit of these records was to determine if there was any correlative evidence of the perceived drop in incidents at the club since the installation of the Vigilance [software] compared to before the installation. An entry in the log was counted as an incident if either a person was removed from Wild Coyote after being admitted or they were involved in an altercation in the WCC parking lot after exiting the WCC.

[37] Wild Coyote, second submission, p. 2.
[38] Wild Coyote, initial submission, p. 2.

> [45] A review of the incident log revealed that, from February 10, 2004, until June 10, 2004, (I arbitrarily chose June 10, 2004 as the implementation date for the purposes of this audit) there were 13 recorded incidents at the WCC. From June 11, 2004, until November 10, 2004, there were 50 incidents. The WCC stated that the logs and how accurate, up-to-date or detailed they were detailed [*sic*] depended largely on the author at the time, which frequently changed because of staff turnover. The WCC believes that the introduction of the system compelled its staff to be more detailed and thorough when completing the written incident log. Records of incidents would now have to be kept in two places (*i.e.* the log book and the system) which allowed WCC management to better audit its door staff and, consequently, produced more complete incident log book entries.
>
> [46] It is also noteworthy that, after the Vigilance software was installed, two people were refused entry that had previously been banned from the WCC while another customer managed to sneak back into the club after being removed that same night. … The WCC contends that the system's effectiveness increases as the size of the database increases.

[67] The actual evidence as to incidents thus suggests that there has actually been at least some *increase* in such events after the installation of the software. While improved reporting may account for some of the increase in incidents, the fact remains that Wild Coyote could not point to a single objective indicator to demonstrate improved safety as a result of the use of the system.

[68] Nevertheless, as the following summary of their submissions indicates, many of the interveners hold, and vigorously advance, strong opinions about the necessity and efficacy of the TreoScope system in addressing violence and the potential for violence, which they say is endemic to at least some establishments.

Barwatch

[69] In its submissions, Barwatch states that it is a non-profit advocacy organization "mandated to provide safe and secure environments to patrons visiting its member establishments", which is of course a laudable mandate.[39] Barwatch explains its origin as follows:

> Barwatch was created in response to the growing safety issues facing the nightlife industry. Violent assaults, weapons, drug dealing, sexual assaults, underage drinking, drink tampering, property damage are just a few of the security concerns facing nightlife establishments. These issues had begun to spin out of control and in response law enforcement agencies and the City of Vancouver began to crack down on operators with high fines, climbing insurance premiums, and closures. It was these circumstances that led nightclub and bar owners and law enforcement to form Barwatch.[40]

[39] Barwatch initial submission, p. 1.
[40] Barwatch second submission, p. 1.

[70] Barwatch is about much more than the use of licence scanning technology such as TreoScope's system. Barwatch sets a number of requirements for member establishments, including use of metal detection equipment and surveillance cameras, in addition to use of TreoScope's ID scanning system. Barwatch's board of directors has vetted several ID scanning systems for its members since 2002 and, its submissions say, only TreoScope's system satisfied its two criteria of being customer-friendly and, in its view, PIPA-compliant.[41]

[71] Barwatch notes that, as an intervener, it was not able to provide evidence other than opinions. As the author of the submission, the Vice Chair of Barwatch, says:

> Personally, as a forty year veteran of the nightlife industry and as a published authority on "Ensuring Public Safety" I can say with absolute certainty that TreoScope's software is the best tool I have encountered in terms of ensuring a safe and secure environment. …In addition, we continually here [sic] about the software catching flagged customers, known gang members, and individuals with court ordered curfews and restrictions from gaining entrance.[42]

[72] Barwatch's submissions say that the "vast majority" of nightclubs in the Greater Vancouver Regional District—also known as Metro Vancouver—use the TreoScope technology and all of the licensed establishments in Vancouver's Entertainment District are currently using it. Barwatch also notes that the public has not stopped frequenting these bars, but rather has expressed gratitude for the software being in place.[43]

ABLE BC

[73] ABLE BC is an industry association representing the interests of liquor licence holders in British Columbia. Its submission says this:

> Liquor Licensees that use the [TreoScope] system tell us there was a noticeable difference in their establishment as soon as they started using it. People that are out to cause a disturbance are less likely to enter an establishment that uses a gateway security system. They are also less likely to cause a disturbance knowing that both their name and photo is on file and can be passed on to law enforcement officials. Barwatch and the Vancouver Police Department had made no secret of their desire to keep

[41] Barwatch second submission, p. 3; Barwatch initial submission, p. 2.
[42] Barwatch second submission, p. 4. It is not stated how the scanning system's operators know when an individual having a court-ordered curfew enters the establishment. This is information that presumably could only come from police or other public body sources.
[43] Barwatch reply submission, p. 3.

> known gang members from entering bars, this system is one tool to help meet that important public safety goal.
>
> … Owners that use the TreoScope system are clear; this system is the single biggest factor that has improved safety in their establishments.[44]

Liquor Branch

[74] The Liquor Branch's submission says this:

> Violence in and around establishments has been increasing in recent years. Based on information relayed by our police partners, the use of weapons in conflict situations is increasing. … It is recognized that liquor impairs judgment and the combination of violence and liquor can lend itself to very dangerous situations for licensees, customers and the public.[45]

[75] The Branch says it can impose certain security measures as a term of liquor licences. It has required one establishment associated with gang activity to use an electronic weapons detection system at the point of entry. As I noted earlier, another bar with a history of both gang violence and minors being present is required to use both a weapons detection system and ID scanning, with the bar being required to keep information collected by the scanning system for one week for use by police and liquor inspectors.[46]

TreoScope

[76] TreoScope's submission notes that the Liquor Act requires operators of licensed establishments to: not permit customers to become intoxicated; not permit anyone to enter with a firearm, knife or other weapon; and to guard against violent, disorderly, riotous or unlawful conduct of customers within their premises (and, arguably, in the vicinity of their premises). TreoScope also says the Liquor Regulation requires bars and nightclubs to record any incidents or events that occur in or adjacent to their premises.[47]

[77] TreoScope says its system falls within the best practices for nightlife establishments developed by the New York Police Department and that both Vancouver and Toronto are considering making ID scanners mandatory for all night life establishments.[48]

[78] Without its system, TreoScope says, bar employees must rely on memory and written notes, or photocopied IDs, to identify problem customers or

---

[44] ABLE BC's initial submission, p. 4.
[45] Liquor Control and Licensing Branch submission, para. 7.
[46] Liquor Control and Licensing Branch submission, para.3
[47] TreoScope second submission, para. 29.
[48] TreoScope second submission, paras. 33 and 36; Affidavit of Owen Cameron, paras. 15-17 Exhibits"F", "G" and "H".

customers involved in incidents in order to prevent re-entry or to assist law enforcement personnel. It says such systems are difficult to implement and maintain and are open to abuse or inappropriate use, with no audit trail for inappropriate access to customers' personal information.[49]

[79] TreoScope submitted two customer testimonials. I have already mentioned the testimonial relating to an establishment that was able to establish a due-diligence defence when a minor was found to be drinking there. This is the entirety of the second customer testimonial:

> I have been in the nightclub business for 14 years and I have to say that the results from using TreoScope EnterSafe are outstanding. Since we began using EnterSafe we have seen a significant decrease in unwanted customers and also property damage.[50]

Chiefs' Association

[80] The Chiefs' Association asserts this in its one-page initial submission:

> The type of information collected by Wild Coyote Club, using the Vigilance Software system, has assisted to solve violent crimes such as stabbings shootings, and other serious assaults, and also has acted as a deterrent with respect to these activities.

[81] The Chiefs' Association's reply submission is somewhat more detailed. It says that, in the experience of Vancouver Police Department ("VPD") members, gang members or others who behave violently will avoid an establishment that requires customers to provide identification and have it scanned into a database.[51] It says that, based on the experience of VPD members and their conversations with those affiliated with gangs:

> It is not unreasonable to conclude that the ability to collect identifying information of nightlife establishment customers is often all that is required to deter some of those who intend to engage in criminal acts inside the establishment.[52]

[82] The VPD has compared the number of incident reports associated with Wild Coyote in 2007 to those associated with "another downtown nightlife establishment that did not use the TreoScope system", noting that there were significantly more incidents at the establishment which did not use the software.

---

[49] TreoScope second submission, paras. 44-45.
[50] Affidavit of Owen Cameron, Exhibit "E".
[51] BCAMPC reply submission, para. 5.
[52] Chiefs' Association reply submission, para 5.

This said, as the submission itself acknowledges, several variables could affect those numbers.[53]

[83] The Chiefs' Association's reply submission also offers this conclusion:

> In consideration of the safety and security challenges faced by Wild Coyote Club, specifically, and British Columbia night club establishments generally, the collection, use and disclosure of personal information facilitated by the TreoScope system is demonstrably necessary to provide for a safe and secure environment.[54]

[84] The reply submission includes a memo from the VPD's Youth Gang Squad, which says that those who go to downtown bars and restaurants are exposed to a substantial risk of violence associated with gang members. The memo's author says numerous nightclub door employees have told him they have a 'no-hands-on' policy with gang members. This is to say that gang members are not searched because a failure to show proper respect could result in serious assaults on them or in their being targeted for shooting.[55] The memo does not say nightclub door staff have been assaulted or shot because they searched gang members, but it speaks to a concern of some risk this might happen.

Analysis

[85] It is troubling that, despite the repeated assertions that TreoScope's system has dramatically improved safety and security, no material such as statistics has been presented that persuasively demonstrates an actual reduction in violent incidents in the Wild Coyote

[86] Section 73 of the Liquor Act requires licensees to produce prescribed records to an inspector on demand, with s. 34(j) of the Liquor Regulation prescribing for this purpose "records of any incidents or events that occurred in or adjacent to the licensed premises". In light of this, it is reasonable to conclude that evidence of numbers of incidents before and after adoption of the TreoScope system could have been produced in order to demonstrate the system's claimed efficacy in reducing numbers of incidents.

[87] According to Wild Coyote, however, it would be more appropriate for expert opinions and data on the need for security systems to come from the VPD, rather than relying on the records of one small business. While I appreciate that Wild Coyote may not be able to produce city-wide statistics, I would have thought that, in light of its above-described incident-logging and reporting obligations under the Liquor Act and Liquor

[53] Chiefs' Association reply submission, paras. 8-11.
[54] Chiefs' Association reply submission, para. 14.
[55] Chiefs' Association reply submission, Appendix A, p. 2.

Regulation, it would have been able to provide some level of detail about the claimed reduction in actual incidents in its own establishment. It is after all, the establishment whose practices and experience are under review in this inquiry. As I noted earlier, Wild Coyote originally asserted an 80% reduction in violent incidents, but this was an estimate only, one that on further investigation turned out to be inconsistent with Wild Coyote's own incident logs.

[88] The only other material of assistance is the submission of the Chiefs' Association. As indicated above, the Chiefs' Association's submissions offer the views of unidentified members of the VPD, and the opinion of the Chiefs' Association, that systems to identify customers deter violent individuals from entering licensed establishments. As noted above, from this, the Chiefs' Association expresses the opinion that collection, use and disclosure of customers' personal information is "demonstrably necessary" to provide for a "safe and secure environment."[56] The Chiefs' Association's submissions do not speak to alternative measures to provide safe and secure environments for patrons.

[89] As an aside, it is reasonable to think that TreoScope itself would have data to support the claims it makes for its product. It has asserted that its clients "report an approximate 75% to 85% drop in violence on their premises through the use of TreoScope technology". Yet it refers only to two customer testimonials in support of these figures. Without specifying claimed percentage decreases in violence, these testimonials offer opinions, not data, to support the claim that security-related incidents have decreased through use of the technology.

[90] In Alberta Order P2006-11[57] ("*Penny Lane*"), Commissioner Frank Work held that the collection of personal information through the scanning of driver's licences on entry to a nightlife establishment was not reasonable. The organization had made this submission:

> The SC system, as part of the overall comprehensive security system, is intended to act as a deterrent to potential wrongdoers in that all customers know that their identification is scanned and that therefore they could easily be identified if they were involved in any violent or illegal activity. It is submitted that potential wrongdoers would be less likely to engage in violent or other illegal behaviour if their ability to remain anonymous was removed.[58]

---

[56] Chiefs' Association reply submission, para. 14.

[57] *Re Penny Lane Entertainment Ltd., Penny Lane Entertainment Group, Tantra Night Club Inc*. [2008] A.I.P.C.D. No. 149; Judicial Review application dismissed, *Leon's Furniture Limited v. Sharon Curtis, The Information & Privacy Commissioner, et al* (18 June 2009), Calgary No. 0801-12471 (Alberta Q.B.); *Penny Lane Entertainment Group v. Alberta (Information and Privacy Commissioner)*, [2009] A.J. No. 300; 2009 ABQB 140.

[58] As quoted in Order P2006-11, [2008] A.I.P.C.D. No. 49, para. 26.

[91] Commissioner Work concluded as follows:

> From my review of the evidence and the parties' submissions, I find that, at best, the Organization offers conjecture that collecting driver's licence information of customers may act as a deterrent to violent behaviour. The Organization did not submit any evidence to establish that collecting the Complainant's driver's licence information, or that of other customers, is in any way a deterrent to violent behaviour. In addition, it did not provide any evidence regarding the causes of violence in bars or statistics relating to the incidence of violence in bars before and after the implementation of a driver's licence collection program. I draw the inference that the Organization is unable to produce any evidence to draw a correlation between violence, customer safety, and collecting driver's licence information. As a result, the Organization has failed to establish any reasonable relationship between collecting driver's licence information and any of its stated purposes for scanning driver's licences. I am therefore unable to conclude that the Organization has a reasonable purpose within the meaning of section 11 when it scans customers' driver's licences.[59]

[92] Similarly, the case summary from the PIPEDA complaint regarding Canad Inns says this:

> Regarding the second stated purpose for using the ID machines (i.e. security) the Assistant Commissioner understood the reasons for ensuring the security of patrons and staff, but did not consider the machines capable of fulfilling this role. Deterrence appears to be an inherent element in the security purpose—namely, the idea that troublesome individuals are less likely to try to enter the beverage room if they know that the identification they present is being recorded. The Assistant Commissioner noted that, while this is certainly possible, there was no way of knowing whether this has ever occurred, and the company could not provide any statistics to support such a hypothesis. Moreover, she noted, identification of VIP members is not usually scanned, so a certain proportion of the clientele would be systematically eliminated from any statistical analysis. Without any evidence to support the claim, it was unclear to the Assistant Commissioner how the ID machines were effective in meeting the need for security.[60]

[93] I accept that the purpose of providing a safe environment for customers and staff is directly related, indeed integral, to Wild Coyote's supply of a product or service. It is not at all clear, however, that the collection and storage of information by the TreoScope system actually plays a significant role in achieving

---

[59] At para. 31. As several of the interveners pointed out here, the system in issue in *Penny Lane* apparently differed from TreoScope's. According to Barwatch, the system utilized in the Alberta case allowed for complete access to and manipulation of all data recorded in the scanned ID, had no personal information retention policy, offered no encryption or protection around databases, and did not provide for audit trails. In addition, the company that developed the system did not provide a privacy policy or signage in order to give notice. Barwatch submission, paras. 15-17.

[60] PIPEDA Case Summary #396, [2008] S.C.C.P.V.P.C. No. 9.

that purpose. While there have been repeated assertions by Wild Coyote that the use of the TreoScope system has improved customer and staff safety, the evidence regarding the number of incidents, from Wild Coyote's own incident reports, is to the contrary. I have considered the content of the Chiefs' Association's submissions, but am not persuaded that it establishes that collection of personal information of all customers of a scope and in the manner in issue here fulfills a significant role in enabling the Wild Coyote to achieve the customer safety purpose.

[94] Nor is there material before me that persuasively addresses whether there are less intrusive alternatives to collection of personal information from driver's licences. Among other things, I note that Barwatch's program entails use of video surveillance and other security measures, with security staff being a traditional means of protecting customers.

[95] As I said earlier, in assessing whether collection of information is "necessary", it is appropriate to state the purpose sought to be achieved as precisely as possible, yet the objective of 'improving customer safety' is generalized. It is not surprising, perhaps, that the submissions that suggested this generalized objective was being achieved were vague about how this was being done.

[96] There appear to be two specific ways in which the TreoScope system might conceivably lead to improved security. First, the VPD's evidence suggests that simply recording customers' identifying information on entry will discourage more violent customers, particularly gang members, from entering. Yet I note that, according to the VPD memo attached to the Chiefs' Association's submission, gang members are known to intimidate door employees into not requiring them to pass through metal detectors.[61] It is not at all clear to me why the same problem would not occur with ID scanning. If gang members avoid scanning for weapons using intimidation, why would they acquiesce to having their licences scanned? Again, there is no objective evidence that persuasively demonstrates any actual decline in gang-related violence as a result of utilizing the TreoScope system.

[97] Second, the Chiefs' Association's evidence also suggests customer safety is improved if an establishment is able to effectively exclude those who have previously been ejected from an establishment.[62] The most specific evidence regarding violence at Wild Coyote is as follows:

[61] As noted above, use of metal detectors is one condition of an establishment's participation in the BarWatch program.

[62] Keeping a record of patrons who have been banned from Wild Coyote was identified as one of the purposes of the collection in the Investigation Report. However, it is convenient to consider it here as part of the purpose of providing a safe environment for patrons.

> VPD members report that prior to adopting the TreoScope system, the violence and potential for violence at that club was substantial. VPD members report that it was necessary for Wild Coyote Club to take extra measures to ensure that persons who had previously engaged in violence at that club, or who had been escorted out of the club by Police members, were carefully scrutinized before being permitted access to that establishment. VPD members report that if violent individuals are barred from entering a nightlife establishment, the customers of that establishment are safer.[63]

[98] This is evidence that it is necessary, in order to preserve a safe environment for customers, for Wild Coyote to be able to identify, in some fashion, those individuals who are determined to be undesirable for re-entry. As a result, I accept that it is necessary for Wild Coyote to be able to collect and use information in order to maintain a record of banned customers. I am not persuaded, however, that it is "necessary" to develop and maintain a personal profile containing the personal information of *all* customers in order to effectively track the few who may be removed from, and subsequently barred from re-entering, an establishment. Certainly, the full scope of information which is collected by Wild Coyote and the length for which it is retained is not necessary to achieve that purpose. As a result, a requirement for consent to the collection of personal information through the TreoScope system is a requirement for consent to the collection and use of information "beyond what is necessary" for providing the service of operating a nightlife establishment in the terms I have described.

[99] For these reasons, I find that the collection of customer information through the use of the TreoScope system, as described in this decision, is not "necessary" within the meaning of s. 7(2) of PIPA. I also find that it is not necessary to collect and retain the physical IDs of patrons in order to operate a nightlife establishment. For reasons given above, there was no persuasive evidence presented to me which demonstrated that such a requirement would have any significant effect on customer safety. While it may make it easier to identify those who are ejected from an establishment, there was no explanation of how this would be done in a PIPA-compliant manner.

[100] Accordingly, Wild Coyote cannot *require* an individual to consent to the collection, use or disclosure of personal information, either through the TreoScope software or through retaining ID during the period of a customer's visit as a condition of supplying a product or service.

[101] **3.3 Deemed Consent to Collection**—The first question set out in the Amended Notice of Written Inquiry is whether the complainant is deemed, in accordance with s. 8(1) of PIPA, to have consented to the collection of his personal information. Section 8(1) of PIPA reads as follows:

---

[63] The Chiefs' Association reply submission, para. 7.

> 8(1) An individual is deemed to consent to the collection, use or disclosure of personal information by an organization for a purpose if
>
> (a) at the time the consent is deemed to be given, the purpose would be considered to be obvious to a reasonable person, and
>
> (b) the individual voluntarily provides the personal information to the organization for that purpose.

[102] As noted above, Wild Coyote says it collects personal information in order to improve customer safety, prevent minors from entering, keep a record of banned customers and keep a record of customers for use in court actions or for law enforcement purposes. However, I note that the TreoScope system does more than enable a record to be kept of customers who have been banned—it also enables the creation and maintenance of a customer profile for all customers and Wild Coyote uses it for this purpose.

[103] I also note that the TreoScope materials offer other reasons for which organizations might want to collect the customer information at issue in this case. For example, the website materials submitted by TreoScope say that the system, "Recognizes your VIPs so you can give them the special treatment and welcome they deserve."[64] TreoScope says the Familiarity Index is important for safety purposes because it indicates whether security staff should watch a particular customer more carefully. For example, if a customer has visited the bar 20 times in the last year and there are no notes about a previous incident involving that customer, security staff believe they have less reason to closely scrutinize that customer's behaviour.[65]

[104] Not all of the purposes for which Wild Coyote collects the personal information in question would be obvious to a reasonable person. While it might be obvious that ID is examined to verify the age of customers, it would not be obvious to a reasonable person that the information is being collected for the purpose of sharing it with law enforcement officials or to create a customer profile that will be updated with each visit occurring within a six-month period. I find that Wild Coyote cannot rely on s. 8(1).

[105] **3.4 Did Wild Coyote Give Adequate Notice?**—The next issue is whether Wild Coyote gave the complainant proper notice of the purposes for which Wild Coyote was collecting the complainant's personal information. Section 10(1)(a) of PIPA says that, on or before collecting personal information from an individual, an organization "must disclose to the individual verbally or in writing ... the purposes for the collection of the information".

---

[64] Affidavit of Owen Cameron, Exhibit "A", p. 1.
[65] Investigation Report, para. 22.

[106] In addition, s. 8(3) provides that an organization may collect, use or disclose personal information about an individual for "specified purposes", but only if the conditions of ss. 8(3)(a) through (d) are met. The first condition is that the organization must provide notice that it intends to collect information for the specified purposes. [66]

[107] Wild Coyote provided the following notice to customers at the time the complainant went to the club:

> Entering Wild Coyote is considered permission to swipe your I.D. and take your picture. This is for security and identification purposes only. Your information will not be shared or used for marketing purposes. Refusal to produce proper I.D. may result in denied entry.

[108] In its initial submissions, the BCCLA took issue with this notice, submitting that it should specifically refer to the information being stored for post-incident investigation.[67] The notice Wild Coyote now uses adopts much of the language that the BCCLA suggested:

> Vigilance Software and this establishment are committed to protecting the environment within this establishment, the individuals who patron [*sic*] it, and the information necessary for safeguarding it. As providing this service involves the collection, use and disclosure of some personal information about our customers, protecting their personal information is one of our highest priorities.
>
> In the event of a criminal or other event in the premises, a police or other investigation may be required. To assist in such an investigation, this establishment wishes to collect and store the following personal information on a TreoScope ID Scanning Station for up to two years: Name; Government ID Number; Expiry Date: Birth Date; Gender and Live Photo. Your address will not be collected or stored and none of your information will be used for direct marketing purposes.
>
> Should an incident occur in which an investigation or communication of your information be required, this establishment may use or disclose your personal information to the police, other establishments, or the investigating body and you may be contacted as a potential suspect, witness or other relevant source of information in an investigation.
>
> If you have legitimate concerns about having your information collected, communicated, and stored by this establishment, please ask to speak to a manager or this establishment's privacy officer for alternative options to gain access.[68]

---

[66] Another condition is that the collection must be reasonable, a matter which is discussed below.
[67] BCCLA initial submissions, para. 30.
[68] Investigation Report, Appendix 2.

[109] This much more detailed and forthcoming notice is a definite improvement. That said, the notice suggests that the information will only be used in "the event of a criminal or other event in the premises" when "a police or other investigation may be required." This may suggest that the information will not be used unless some significant event occurs. Moreover, even the new notice fails to say that a customer's information will be used to create a customer profile and that the technology will be used to verify the authenticity of customer ID.

[110] Neither the notice in place at the time of the incident nor the notice currently in use gives full disclosure of the purposes for collection of personal information. Because the notice did not disclose all of the purposes for the collection of the information, I find that Wild Coyote was not in compliance with s. 10(1)(a). Failure to give notice of all of the purposes of collection is also enough for me to decide that Wild Coyote cannot rely on s. 8(3) and I so find on this basis.[69]

[111] **3.5 Appropriate Collection in the Circumstances?**—I have held that the personal information collected is not "necessary" in order for Wild Coyote to provide the service of operating a licensed establishment. As a result, Wild Coyote cannot require the information as a condition of entry into Wild Coyote. However, it may still be reasonable for Wild Coyote to collect the information from those of its customers who consent in accordance with PIPA.

[112] Section 11 of PIPA reads as follows:

> Subject to this Act, an organization may collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> (a) fulfill the purposes that the organization discloses under section 10(1), or
>
> (b) are otherwise permitted under this Act.

[113] In *Gostlin*, I addressed s. 11 this way:

> Under s. 11, one has to decide whether the hypothetical reasonable person, knowing the purposes for collection and the surrounding "circumstances", would consider the purposes for collection to be "appropriate". Relevant circumstances may include the kind and amount of

[69] The complainant has said that he was not given an opportunity to decline to have his ID scanned. When this Office's investigating Portfolio Officer visited Wild Coyote, he was given an opportunity to refuse to have his ID scanned, but he was refused entry as a result. Of course, in order to rely upon s. 8(3), the individual must be given an opportunity to decline to provide the information.

> personal information being collected, the uses to which it will be put and any disclosures the organization intends at the time of collection.[70]

[114] Under the system currently in place, the personal information that is collected by the TreoScope software is the patron's name, photograph, date of birth, sex and driver's licence number. Only the first three are available for use or disclosure by Wild Coyote. The system also collects a partial postal code. However, because the partial postal code is not linked to the other information, it is not information about an identifiable individual and so is not personal information.[71]

[115] In its submissions, TreoScope says it "cannot access the data base unless it is subject to a judicial warrant or it does so to maintain, update or upgrade the System software."[72] I am not certain that it is accurate to say that TreoScope "cannot" access the information without a warrant. The affidavit referred to in the submissions says this:

> TreoScope cannot view, print, email, or copy any personal information on the System by Wild Coyote without gaining access to their local system housed on nightclub premises, which offers a second check and balance in ensuring the information is protected.[73]

[116] While TreoScope may decide not to access the information unless one of its customer establishments is subject to a warrant or disclosure order, it seems quite clear that TreoScope could do so in other cases.

[117] I have previously held that an individual's name, address and telephone number are, generally speaking, of a non-sensitive nature.[74] One's sex, as recorded on a driver's licence, is also not usually considered sensitive information. In the context of a visit to a licensed establishment, I would also find that one's age is not sensitive because it is understood that it may be necessary to disclose it, at least where there is some reasonable question about whether the individual is of legal drinking age. An individual's date of birth and driver's licence number are more sensitive, not because they reveal any particularly personal details about an individual, but because they are often used to verify identity.

[118] This Office last year issued a joint statement, with the Office of the Information and Privacy Commissioner of Alberta and the Office of the Privacy Commissioner of Canada, about the sensitivity of driver's licence numbers due to their value in facilitating identity theft. This statement makes clear that driver's licence numbers should not be collected where an examination of the licence

---

[70] At para. 55.
[71] Investigation Report, para. 15.
[72] Treoscope initial submission, para. 40.
[73] Affidavit of Owen Cameron, para. 6.
[74] *Gostlin*, para. 58.

itself is sufficient.[75] As set out in Investigation Report P2007-IR-006, jointly issued by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of Alberta ("*Winners*"),[76] the risk of inadvertent disclosure of information such as driver's licence numbers can have serious consequences.[77] As a result, the collection of this kind of information should be limited to when it is truly required.

[119] In addition to the initial collection of information upon entry to the establishment, the use of the TreoScope software also involves the collection of information about an individual's activities, for example, how often he or she attends the establishment and any activities in which he or she engaged, which are the subject of notes added to the profile by bar staff. This may, in some circumstances, be considered sensitive information. Of course, it is information which would be available to anyone simply observing and recording a patron's activities. In that sense, it is not in any way confidential. However, the ease of electronic recording of this kind of information means that it is amassed and analyzed much more readily than it would be through personal observation. The comprehensiveness of this collection makes it more intrusive than collection by physical observation.

[120] In addition, it is important that the information is to be stored for a significant period of time. The Court of Appeal for England has recently recognized that, even when it is reasonable for the police to take photographs for the prevention of disorder or crime, the retention of such photographs must be justified. Dyson LJ noted that, "The retention by the police of photographs taken of persons who have not committed an offence, and who are not even suspected of having committed an offence, is always a serious matter."[78] The retention of personal information regarding the whereabouts and activities of individuals by an organization, with the stated purpose of providing such information to the police, also raises privacy concerns.

[121] As set out above, a number of purposes are advanced for the collection of information—to provide a safer environment for patrons, to prevent minors from entering the premises, to keep a record of patrons who have been banned from Wild Coyote and to keep a record of patrons in case the information is needed in a court action or by law enforcement officials. It is necessary to consider both whether these purposes for the collection are reasonable and whether the collection fulfills these purposes in determining whether the collection complies with s. 11.

---

[75] "Collection of Driver's Licence Numbers under Private Sector Privacy Legislation: A Guide for Retailers", available at http://www.oipc.bc.ca/pdfs/private/guide_edl_e.pdf, p. 4. See also *Re Home Depot of Canada*, [2008] A.I.P.C.D. No. 29, and P.I.P.E.D.A., Settled Case Summary #16.
[76] [2007] A.I.P.C.D. No. 34.
[77] [2007] A.I.P.C.D. No. 34.
[78] *Wood v. Commissioner of Police for the Metropolis,* [2009] EWCA Civ 414.

To prevent minors from entering the premises

[122] Given that nightlife establishments are responsible for ensuring that minors do not enter their premises, I find that it is generally accepted that there may be a collection of some of the personal information associated with a driver's licence upon entry to a nightlife establishment, in order to ensure that a patron is of legal drinking age. However, just as the cases involving the return of merchandise have drawn a distinction between examining a driver's licence to establish identity and actually recording the driver's licence information, there is a significant difference between door staff examining ID to establish that a patron is of drinking age and actually recording the driver's licence number and other information. I recognize that the terms and conditions of the establishment's liquor licence suggest that it may be appropriate to record the driver's licence information in some circumstances. However, the TreoScope software collects that information for all customers, regardless of their apparent age and any other circumstances.

[123] Where there is some question about whether a patron is of legal drinking age, it may be reasonable to scan a piece of identification in order to verify its authenticity and to generally ensure that the patron is of legal drinking age. However, this purpose is not furthered by actually recording the information embedded in the card and retaining it. In addition, much of the information collected by the TreoScope software does not fulfill the purpose of ensuring that minors are prevented entry. For example, this purpose is not served by the collection and retention of the driver's licence number or by scanning the IDs of those individuals who are clearly of legal drinking age. Thus, in considering the scope of the information collected by the TreoScope software, I find that its use is not reasonable or appropriate for this purpose within the meaning of s. 11.

To provide a safer environment for its patrons

[124] As set out above, the two specific ways in which the collection of personal information through the TreoScope system can be said to further the purpose of improved customer safety are by preventing the entry of those individuals likely to be violent and by assisting Wild Coyote to identify those individuals who are not suitable for re-entry. Wild Coyote and some interveners suggest that the TreoScope system will also improve customer safety because individuals will be less likely to cause trouble if they know that their personal information is held and that therefore they can be identified. I am not persuaded that this is necessarily the case. In *Gostlin*, the evidence established that the fraudulent return of goods had become a "sophisticated illegal business operation" which resulted in significant losses to the organization. Those who are engaged in such an operation may indeed change their behaviour based on an understanding that they can be identified. It is much less clear that an individual who becomes involved in an altercation while drinking will consider the implications of the fact that his ID was scanned when he first entered the establishment.

[125] Is it reasonable for Wild Coyote to use the TreoScope software to collect customer information in order to deter entry of those likely to be violent and to prevent re-entry by those who do cause trouble? In this regard, I find that the statutory framework in which licensees operate is relevant. As noted by TreoScope, the Liquor Act imposes on licensees significant obligations in terms of ensuring that they do not permit their patrons to engage in "gambling, drunkenness or violent, quarrelsome, riotous or disorderly conduct."[79] The statute also provides licensees and their employees with the statutory authority to request a person to leave, or forbid a person to enter, a licensed establishment if the licensee or its employee believes that the presence of the person in the establishment is undesirable.[80] It is an offence for a person to remain in a licensed establishment when requested to leave by the licensee or to attempt to re-enter within 24 hours of being asked to leave.[81]

[126] These provisions demonstrate a recognition by the Legislature that, because licensees have considerable responsibility for the behaviour of their patrons, they must be able to exercise some discretion regarding who is allowed to enter their premises. As discussed above, other parts of the regulatory framework contemplate an examination of identification, at least for those who may not be of age.

[127] I find that it is reasonable, in the case of Wild Coyote, for it to be able, in order to preserve a safe environment for customers, to identify those individuals who have been determined to be violent, or otherwise undesirable for re-entry from a safety perspective, and thus improve customer safety. However, much of the information collected by the TreoScope system does not further this safety purpose. Moreover, I have not been provided with any reason related to improved customer safety for an establishment's retention of any information at all relating to customers who are not involved in violent incidents. The so-called Familiarity Index is privacy-intrusive and I am not persuaded that it has any material value for improved safety.

[128] In its submissions, ICBC noted that Treoscope had stated that the collection of a patron's driver's licence number was necessary in order to assist law enforcement in differentiating between two people with the same name. ICBC suggested this could be done through comparisons of photographs and birth dates.[82] In reply, TreoScope said this:

> In this regard, it is important to point out that the software which operates TreoScope's System will not work without a driver's licence number. A driver's licence number is a true unique identifier. In other words, no one

[79] Liquor Act, s. 36(2)(a).
[80] Liquor Act, s. 46(1).
[81] Liquor Act, s. 46(3)(a), (b).
[82] ICBC submissions, p. 2.

> else has the same driver's licence number. However, people can share birth dates and photographs cannot be reliably matched to a birth date. In order to have certainty that a person has entered a bar or nightclub a driver's licence number is determinative of the issue and can conclusively confirm the identification of a person.[83]

[129] It is not entirely clear what point TreoScope is making in this response. If TreoScope is saying that the software is designed to use the driver's licence as a unique identifier in order to organize the other information, it is not clear why this could not be achieved by some other method, such as cross-referencing the name and date of birth of customers. In any case, given that I have found that it is not necessary to retain information other than that necessary to identify banned patrons, it is not clear that a unique identifier is required. I note that, even when a unique identifier is required, it is preferable for a system to immediately assign an identifier other than a driver's licence number in order to organize the information, as was done in *Winners*. If TreoScope is saying that the driver's licence number is required to assist law enforcement agencies, that purpose is addressed below.

[130] Again, considering especially the scope of personal information collected and the manner of collection, that is, by recording it for retention for two years, I find that the use of the TreoScope system is not reasonable or appropriate, within the meaning of s. 11, for the purpose of improving customer safety.

[131] I did not receive any submissions from TreoScope or Wild Coyote which would indicate that the software could be used to only collect information necessary to achieve the purpose of identifying banned individuals when they seek re-entry. Wild Coyote's further supplemental submissions did include the following statement:

> I should also note that in August 2008, TreoScope updated our software with the ability to delete a customer from our system. A future alternative may be to initially scan an individual – thus gaining access to the authenticity and prior misconduct checks – and then remove the customer from this system, while they watch; at the end of the night, should no incident occur that involves them.

[132] Of course, I have received no submissions from the other parties on this alternative, and no details from Wild Coyote on how the system would operate if it were aimed at only maintaining a list of banned customers. As a result, I can only decide whether or not the collection as a whole, as it was being conducted at the time of the Investigation Report, complies with s. 11 of PIPA. For reasons already given, I conclude that it is not. The alternative proposed in Wild Coyote's supplemental submissions would likely involve different considerations and cannot be addressed here.

---

[83] TreoScope reply submission, para. 16.

Record of patrons for court actions or helping police investigations

[133] It appears from the submissions of Wild Coyote, TreoScope and the interveners that this is the purpose that requires, they say, retention of the driver's licence number and which requires customer information to be held for a period of up to two years. It is therefore this purpose which requires the collection of the most sensitive information and which necessitates the development and maintenance of a significant database of all customers' personal information.

[134] I am not persuaded that it is reasonable for nightlife establishments to collect this amount of personal information in order to assist law enforcement in the event that a crime happens to occur. Wild Coyote said that it has been served with two warrants and one production order for information held in its databases.[84] The submission of the Chiefs' Association confirmed this and added:

> The VPD confirms that information legally obtained, via warrant or production order, has successfully aided the VPD in larger scale investigations. For example, with respect to a recent homicide, data legally obtained from a TreoScope system assisted investigators to establish an accurate timeline of events, and also assisted investigators to determine with whom the victims had associated at the nightlife establishments.[85]

[135] The Chiefs' Association said that the TreoScope system "is considered by VPD investigators to be a valuable tool in a criminal court prosecution as it provides actual evidence placing an accused at a particular location at a specific time."[86] The Chiefs' Association responded to a submission by the BCCLA, to the effect that it is unnecessary to keep records for two years, by arguing that it is not uncommon for investigators to seek warrants or production orders several months or even years after an incident takes place. The Chiefs' Association said that, for example, victims of sexual assault may not come forward to police until long after an assault has taken place.[87] There is, however, no indication that information collected by the TreoScope system has ever been used in an investigation regarding sexual assault.

[136] I have no doubt that the police may find the records kept by the TreoScope system to be useful in some circumstances. Indeed, any database—whether private sector or public sector—which tracks the movement or activities of individuals may be of assistance to police in some circumstances. This does not, however, mean it is reasonable to collect and maintain a database of personal information relating to all of the patrons of an establishment for

[84] Wild Coyote Second Submission, p. 3.
[85] BCAMCP reply submission, para. 15.
[86] BCAMCP reply submission, para. 16.
[87] BCAMCP reply submission, para. 17.

a period of two years. In my view, the broad scope of this collection is not appropriate under s. 11.

Conclusion on s. 11

[137] I find that it may be appropriate for the Wild Coyote to collect some personal information from its customers upon entry in order to further the purposes of preventing minors from gaining access and improving customer safety. However, much of the information collected by use of the TreoScope system, such as the driver's licence numbers, does not fulfill these purposes. As a result, Wild Coyote's collection of personal information through the existing TreoScope system is not in compliance with s. 11 of PIPA.

[138] **3.6 Appropriate Use in the Circumstances?**—Section 14 of PIPA reads as follows:

> Subject to this Act, an organization may use personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> (a) fulfill the purposes that the organization discloses under section 10(1),
>
> (b) for information collected before this Act comes into force, fulfill the purposes for which it was collected, or
>
> (c) are otherwise permitted under this Act.

[139] There is no evidence before me about whether or how the complainant's information was used by Wild Coyote. There is thus no need to address this issue.

[140] **3.7 Providing Information About Use of Customer Information**—Section 23(1)(b) of PIPA reads as follows:

> 23(1) Subject to subsections (2) to (5), on request of an individual, an organization must provide the individual with the following: …
>
> (b) information about the ways in which the personal information referred to in paragraph (a) has been and is being used by the organization;

[141] The complainant asked Wild Coyote staff how the information which had been collected from his driver's licence would be used. He was told that his personal information would only be held and accessed by a third-party business that provided the ID scanning system to Wild Coyote. There is no evidence that he was told that his information would be used to create a customer profile or that it might be provided to the police. There is no indication whether any notes were made on the complainant's file or if this was disclosed to him.

[142] The complainant did not contact Wild Coyote after his initial visit in order to request additional information. He indicated to this office that he did not wish to file a complaint directly with Wild Coyote, and he asked for anonymity in the inquiry process.

[143] I find that Wild Coyote staff should have been able to provide the complainant with more information about how his personal information might be used after collection. I find that Wild Coyote did not fulfil its obligation under s. 23(1)(b). I will add in passing, however, that it is always best if a would-be complainant and the organization can discuss these matters directly so that there is more than one opportunity to provide sufficient information.

[144] **3.8 Reasonable Security Arrangements**—The next issue is whether Wild Coyote has met its obligation under s. 34 of PIPA, which reads as follows:

> 34 An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

[145] With respect to physical security, at the time this Office conducted a site visit on April 20, 2007, there was no physical security for the system except for the locked doors of the Wild Coyote. This deficiency was brought to Wild Coyote's attention. It responded by saying it would hire a carpenter to construct an enclosure, so that the system was under lock and key. Wild Coyote has since confirmed to the OIPC that the computer that records all of the personal information remains on site but is now in a fastened and locked metal cage.

[146] The security measures in place are described above. There have been no significant concerns raised by the parties regarding the adequacy of these measures and none are apparent to me on the evidence provided, at least with respect to the encryption of data. I note that I did not receive information from Wild Coyote or TreoScope about what steps are taken to ensure that only authorized staff have access to the system, through, for example, the development and maintenance of user-ID and authentication mechanisms. At this time, I am not prepared to find that Wild Coyote is not in compliance with s. 34, although, if a database is to be maintained, I would encourage Wild Coyote and TreoScope to periodically review all of their procedures to ensure that security arrangements are kept up to date and as secure as reasonably possible.

[147] **3.9 Retention of Personal Information**—Section 35 of PIPA reads as follows:

> 35(1) Despite subsection (2), if an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least

> one year after using it so that the individual has a reasonable opportunity to obtain access to it.
>
> (2) An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that
>
> (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and
>
> (b) retention is no longer necessary for legal or business purposes.

[148] At present, all of the personal information is kept by Wild Coyote or TreoScope for a period of two years. Given that I have held that it is not necessary or appropriate for Wild Coyote to collect the full range of information which is at present collected by the TreoScope system, it is not necessary for Wild Coyote to retain that information for any period. As a general matter, I have held that it may be reasonable for Wild Coyote to collect and retain information necessary to identify those individuals who have been deemed unsuitable for re-entry. However, I have received no submissions on how this might be done, or on how long it would be appropriate to retain this specific information, and so it is not appropriate to address this issue at this time.

4.0 CONCLUSION

[149] For the reasons set out above, pursuant to ss. 52(3)(e) and 52(3)(f) of PIPA, I order Cruz Ventures Ltd., doing business as Wild Coyote Club, to stop collecting and using personal information in contravention of PIPA and to destroy all personal information that it has collected in contravention of PIPA. This requires Wild Coyote to ensure that TreoScope eliminates the database of information which has been collected contrary to PIPA. As a condition made under s. 52(4) of PIPA, I require Cruz Ventures Ltd. to deliver to me an affidavit, sworn by a person with direct knowledge of the matters deposed to, attesting to destruction of the personal information ordered above. That affidavit must be delivered to me not later than 30 days after Cruz Ventures Ltd. has been given a copy of this order.

[150] This Office investigated the complaint underlying this order and, after investigation over a period of time, the matter proceeded to inquiry. As noted at the outset of this decision, having received submissions on the issues, I determined there was not sufficient evidence and argument to enable me to properly consider the merits and make a decision. I therefore referred the matter for further investigation, leading to the Investigation Report. This added to the time taken to bring this matter to conclusion, but the time taken reflects the fact that the issues involved in this case have demanded careful reflection and consideration.

[151] I will close by affirming, strictly in passing and not as part of my decision, that I am well aware of, indeed share, public concern about gang violence and public safety in British Columbia. Some may assert that the technology involved here is synonymous with safety, such that any decision perceived to constrain ID scanning is a decision against safety. These are easy claims to make, but my duty is to apply PIPA based on the evidence and argument actually before me, which I have done.

[152] On the basis of the material before me, I have decided that it is reasonable for Wild Coyote to be able, in order to preserve a safe environment for customers, to identify those individuals who have been determined to be violent or otherwise undesirable for re-entry from a safety perspective, and thus improve customer safety. For the reasons given above, however, the collection of personal information as a whole does not comply with PIPA. In this light, and in view of the reasons given above, I invite—indeed, strongly encourage—those involved to seek the views of this Office if they wish to find a solution for collecting personal information of a nature, and in a manner, that complies with PIPA.

July 21, 2009

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

OIPC File No. P04-21866

Investigation Report on the Wild Coyote Club (Cruz Ventures Ltd.) and its use of Identification Scanning Software from TreoScope Technologies

November 5, 2007

Table of Contents

1.0 INTRODUCTON

[1] This investigation, conducted under section 36(1)(a) of the *Personal Information Protection Act* ("Act"), arose from a complaint initiated by a patron of the Wild Coyote Club (WCC) in Vancouver, BC. The complainant visited the bar on June 12, 2004 and was asked by WCC staff to produce his driver's licence and have it "swiped" through a card reader. The complainant was also required to present for a digital photo. The patron did not receive what he considered a reasonable explanation as to why his personal information was being collected and subsequently complained to the Office of the Information and Privacy Commissioner (OIPC).

2.0 BACKGROUND

[2] On June 12, 2004 the complainant sought entrance to the WCC. The door staff requested his driver's licence, swiped the licence through a card reader and required the complainant to have his photograph taken by a surveillance camera before he would be allowed to enter the WCC. The complainant observed that this requirement was being applied to every patron that entered the premises. He asked if he could "refuse consent" and he was informed by door staff that the ID scanning was mandatory to be granted entrance to the WCC. Before he was given the opportunity to refuse to have his ID scanned, the door staff had already scanned his ID thus collecting his personal information. Seeing that his personal information had already been collected, he entered the WCC. Upon exiting the WCC, the complainant spoke with a man whom he identified as a supervisor, and asked what the purpose of the ID scanner was. The complainant states he was told that his personal information would only be held and accessed by a third party business that provided the ID scanning system to the WCC.

[3] On June 13, 2004, the complainant lodged a complaint with the OIPC under the *Personal Information Protection Act* ("PIPA") about this collection of his personal information. The complaint was assigned to Portfolio Officer Jay Fedorak who conducted an investigation and produced a report of the facts of the case. The report, which included the opinions of the complainant, the WCC and TreoScope[88] (the company providing the ID scanning software) was released to the parties during attempted mediation of the complaint. In his report, Mr. Fedorak provided a description of the ID scanning system, WCC's rational for its usage and the complainant's concerns. The matter was not resolved in mediation and was referred to an inquiry under section 50 of PIPA on November 22, 2005. On March 15, 2007, the Commissioner determined he had not received sufficient information from the participants of the inquiry to make a decision on this case and referred the matter for further investigation.

[88] TreoScope Technologies, Inc.

3.0 PURPOSE OF THIS REPORT

[4] The purpose of this investigation is to:

1. Describe the technology used by the scanning system.

2. Describe:

- The personal information that is collected by the WCC through the system and the process by which that information is collected;
- The purpose of the collection;
- The uses of that personal information;
- Who and under what circumstances the personal information is disclosed;
- The accuracy of the information;
- How long the information is retained; and
- The safeguards that exist to protect the information.

4.0 METHODOLOGY

[5] The following steps were taken in the preparation of this report:

a. A review of the investigation file created by Portfolio Officer Jay Fedorak;

b. A site visit during WCC's business hours was conducted.

c. Interviews with Greg Bell, owner and Privacy Officer of WCC, and Owen Cameron, owner of TreoScope,

d. A review of the material submitted for inquiry purposes by WCC, TreoScope, Barwatch and the BC Civil Liberties Association (BCCLA).

e. A review of the WCC's incident log from January 31, 2004 until November 30, 2004.

5.0 DESCRIPTION OF THE VIGILANCE SOFTWARE SYSTEM ("THE SYSTEM")

[6] The Vigilance Software system is a security product developed and maintained by TreoScope Technologies. The WCC employs the system on

a contractual basis with TreoScope and is dependent on TreoScope for not only the delivery of the system but also technical support and data retrieval.

[7] The system the WCC employs to scan driver's licences consists of a stand alone (not connected to the internet or other computers) computer with a keyboard, mouse, monitor, an ID scanner and a surveillance camera which is used to take still photographs.

[8] As a patron enters the main door of the WCC, the patron is led into a small anteroom in which the WCC door staff asks for ID (usually a driver's licence or a BC ID). Once the door staff have the ID they swipe it through a card reader not unlike the one used a store to make a purchase by debit card. On the right hand side of the anteroom is a small computer, (which is where the information from the magnetic strip on the ID is stored), a computer screen, and (which displays the patron's information each time their ID is scanned). A small camera embedded in the wall a few feet above the computer screen takes the patron's photograph upon entry. This photograph is matched to the information scanned from the ID and stored on the computer. The system also has the capability for an operator, with access authorization, to input notes on individual patrons (also discussed below). After the ID has been scanned the patron is permitted to proceed through another set of doors and enter the WCC premises.

[9] If there is an "incident" at the WCC and the WCC believes there is a need to locate certain patrons in the computer, either to retrieve information for the police or to input notes on a patron's involvement in an incident, then the database can be searched by querying the driver's licence or BC ID number, name, date of birth or by scrolling through the photos. On these occasions, Greg Bell will give the security person access, by logging into the system using his username and password, to scan the photos to identify an alleged offending patron. This process occurs at the end of the night, after patrons have left.

[10] The system permits role based access to the information in the system.

[11] The WCC currently permits door staff to view information on patrons, which includes internal notes and statuses regarding past incidents at the WCC. Greg Bell has the highest level of access, which allows him to not only view this information, but create new notes or statuses on patrons to the WCC.

6.0 PERSONAL INFORMATION COLLECTED

[12] The following personal information is collected through the system:

- photograph
- drivers' licence number
- name

- gender
- date of birth
- partial postal code

[13] The system also records the date and time the patron entered the bar and tracks the number of visits ("familiarity index") for each patron. Essentially, a profile is kept of each patron of the WCC.

[14] The system allows the operator to input notes regarding patrons if the WCC deems their involvement in an incident to warrant such an entry. For example, if a person becomes violent at the WCC and is removed from the premises, then notes regarding the incident can be recorded on the patron's profile. Conversely, if the WCC has a patron that they want to label as a VIP, they can also input that information into the system. The notes can vary in descriptiveness and may range from a few words such as "evicted for fighting" to a several paragraphs, depending on the severity of the incident. Currently there is no written policy regarding what should or should not be included in a note regarding a patron.

[15] The partial postal code that is recorded from each patron's ID is not stored in a manner that is connected to their profile and is used for demographic statistics only. For example, the partial postal codes could be extracted from the system by TreoScope and used to indicate the general areas patrons reside so that the WCC can better target its advertising efforts.

7.0 NOTICE AND CONSENT

[16] The WCC relies on implied consent to collect the personal information. It believes the purpose for which the information is collected is obvious (i.e. to maintain a safe environment within the WCC) and believes so for the following reasons:

- The system is made visible to the individuals prior to their entry into the WCC;

- The reasons for collection are readily displayed in the three signs[89] in the entryway;

- Patrons are given a reasonable opportunity to ask questions or raise an objection prior to being entered into the system; and

[89] Included with the system were three signs displayed to provide notice of the purpose of the system to the public (see Appendix 1). According to Greg Bell and Owen Cameron new signs (see Appendix 2) will be included with the new release of the Vigilance software (TreoScope EnterSafe Gateway Security, released on August 20, 2007, discussed later in this report).

- Patrons voluntarily provide their personal information (by handing over their identification to the door staff) for entry into the system.

[17] It is the WCC's unwritten policy, (which is now written as in Appendix 4), that if an individual has not raised a concern or attempted to opt-out after reading the signage, visually seeing Vigilance Software in use, and handing over their identification for scanning into the software, then the consent is implied. It is also the WCC's policy that if a patron does not possess a scannable piece of ID such as a driver's licence or they are reluctant to have their ID scanned that they can ask to speak to a senior manager who will decide if a person could be admitted, on a case by case basis, without having their ID scanned.

[18] On April 19, 2007, a site visit was conducted, specifically to confirm this policy, in which I attended the WCC and attempted to obtain entry without identifying myself as an OIPC employee. A person working at the entrance asked for my ID so that it could be scanned into the system. I said that I did not want my ID to be scanned, but still wanted to enter the premises. The employee then stated that I would not be allowed entry without having my ID scanned. I was not permitted to speak to the manager.

[19] The following day, an interview with the Manager, Greg Bell, was conducted. He stated that, if a patron does not have their ID scanned, the Manger would hold the ID until the patron leaves the premises. When he was informed of what had taken place the night before, he said he would take immediate steps to correct the practice and to provide the employee with appropriate training to properly handle similar situations in the manner consistent with WCC policy (*i.e.* to contact Mr. Bell himself who would then assess whether or not to admit a patron without scanning their ID).

8.0 PURPOSE FOR COLLECTION

[20] The WCC states that it collects personal information for the following reasons:

5. To provide a safer environment for its patrons;

6. To prevent minors from entering the premises;

7. To keep a record of patrons that have been banned from the WCC;

8. To keep a record of patrons in case the information is needed for a court action involving the WCC or is required by law enforcement to investigate a crime; and

To provide a safer environment for its patrons

[21] The WCC states that its most important reason for having the system in place is to create a safer atmosphere for their patrons. It states that having the system creates a "deterrent effect" for patrons who are likely to cause incidents involving violence, drink tampering or any form of harassment. The WCC believes that if a patron knows that the WCC has a digital photograph of them along with identifying information from their ID, the patron will be less likely to engage in unacceptable behaviour.

[22] Owen Cameron believes that the "Familiarity Index" is important for safety purposes as it indicates whether security staff need to watch a particular patron more carefully. For example, if a patron has visited the bar twenty times in the last year and has no notes regarding a previous incident at the WCC then security staff believe they have less reason to closely scrutinize that patron's behaviour.

To prevent minors from entering the premises

[23] The WCC believes that the system assists them in preventing minors from entering the premises. This, they state, is done through the system's ability to detect fake ID and to prevent minors from "ID passing". When a card is scanned through the system it records information from the magnetic strip on the card. If the card is not properly encoded, the machine will not be able to read it, thus alerting the door staff. Any ID that was originally valid but has been visually altered will record and display the original information on the magnetic strip, alerting the door staff when information on the ID does not match information displayed on the computer screen.

[24] "ID passing" occurs when a patron enters a business such as the WCC with their legitimate ID but, once inside, passes their ID to another person who then passes it to another person outside the business. This person then attempts to use the ID for entry to the business. If a person's ID is used more than once on the same day, the photograph from the first entry attempt is recalled on the system and the door staff will be able to compare that photo to the person standing in front of them.

[25] The WCC has two employees checking ID, one at the door and one just inside to scan the ID and to take the photos. Owen Cameron stated that, from his experience in the industry, most pieces of ID that are passed are either expired or about to expire.

[26] The WCC states that, by recording each person's name and driver's licence / BC ID number as well as taking their photograph upon entry, the WCC is following the suggestion from the Liquor-Primary Licence – Terms and

Conditions (see appendix 5)[90] on how to deter minors. Michael Goodfellow, Policy Analyst at the Liquor Control and Licencing Branch, confirmed that these suggestions have been published and made available to licensees since November 2002.

[27] During the interview with Mr. Bell on April 20, 2007, he admitted that the WCC has not had a substantial problem with infractions under the *Liquor Control and Licencing Act* (LCLA) and could not conclusively state whether the system has had an impact on minors unknowingly entering the WCC. He stated that, based on his experience, the average age of the patron's at the WCC is 19 to 24 years of age so the possibility of minors attempting to access the premises was always a concern. An online search of the Liquor Control and Licencing Branch's enforcement decisions reveals that the WCC has only been involved in two enforcement actions which occurred on December 17, 2003 and June 8, 2004. The two infractions were regarding over crowding and not having the appropriate red lined floor plan available for inspection as required by the LCLA. The WCC was also issued a Contravention Notice on March 1, 2003, for having minors on the premises but no enforcement action was taken.

[28] The WCC believes the system provides important evidence in making a due diligence defence if enforcement action, regarding minors, is taken against them. For example, with information from the system, the WCC will be able to show police and/or Liquor Control Inspectors photographs of every patron they admitted to the bar and proof that their ID was checked. This proof, they believe, will prevent minors from entering the premises therefore preventing possible fines or suspension of their liquor licence.

To keep an up-to-date and accurate log of any patrons who have been banned from WCC

[29] The system allows WCC to keep an up-to-date and accurate log of any patrons that have been banned from WCC for any number of alleged inappropriate behaviours such as fighting or suspected drink tampering. Prior to the system being installed, the WCC relied on the memories of the door staff and a written log to keep track of incidents and banned patrons. As time passes and door staff changes, these methods of tracking banned patrons may become less effective.

[90] The full 43 page version of the Terms and Conditions, "A Guide for Liquor Licensees in British Columbia", can be found at http://www.pssg.gov.bc.ca/lclb/publications/ guides-licensee/LiquorPrimary.pdf

To keep a record of patrons in case the information is needed for a court action involving the WCC or is required by law enforcement to investigate a crime.

[30] The WCC states that, because of the nature of its business, it is possible that it could be involved in a court action from time to time. They believe that the information they collect allows them to better reconstruct events and/or aid them in contacting individuals that may act as witnesses to a specific incident.

[31] The WCC also states that if an offence such as sexual assault occurs on the premises the information could help law enforcement locate and prosecute those responsible, thus adding to the deterrent effect of the system.

9.0 DISCLOSURE OF PERSONAL INFORMATION

[32] The WCC says that it will provide information from its system to law enforcement personnel if ordered to do so via a warrant. However, the WCC also stated that it has verbally provided information to the police without a warrant on several occasions at their request.

[33] The WCC provided anecdotal evidence that the system has decreased incidents of improper behaviour at the WCC. It stated that the system assisted in the investigation of an alleged drink tampering and a high profile kidnapping.

[34] At this time, the WCC does not share information through the system with any other businesses and, as noted above, is not connected to the internet. The WCC states that it has not considered sharing information with other establishments but may consider it in the future. The WCC said that, because it is approximately ten kilometres from the main night club area in Vancouver (mostly located on downtown Granville Street), it does not have the same problem the other bars have with patrons being removed from one bar to only walk down the street and enter another bar and cause similar problems on the same night. Therefore, the WCC does not see much benefit in connecting the system with other businesses that use the same system.

[35] If WCC does decide to implement the information sharing option, then the only way other establishments would be able to see information about one of his patrons was if there were incident notes written about that patron at the WCC and then that person's ID was later scanned at another business that was using the same TreoScope system. For example, this would allow another business to read notes regarding an alleged incident that occurred at the WCC. The business would only be able to view this information if the patron was in front of them seeking entrance into their establishment and the patron used same ID to scan into the system as was used to gain entry to the WCC.

10.0 ACCURACY

[36] The WCC states that it allows individuals to access to their personal information contained in the system as per the access provisions of the *Personal Information Protection Act*. The WCC has confirmed that it will be the first point of contact for any access requests or complaints regarding its system. However, only TreoScope has the required access to the system to correct or print out personal information requested. Therefore, if information needed to be corrected the WCC would have to notify TreoScope who would then access the system and change the information.

11.0 RETENTION

[37] All information is stored for two years from the date of the patron's last entry. The time limit is reset each time the patron visits the WCC.

[38] The WCC says that according to the *Limitation Act* there is a two year time limit within which a patron may seek a remedy from a court where they allege that the WCC is liable for damages for an incident that occurred while on WCC property. They state that, for these purposes, they retain the personal information they collect for two years.

12.0 SAFEGUARDS

[39] The software includes various access levels and, as already discussed above, employees at WCC can only view patron profiles of patrons who are in the club on any particular night. WCC managers have access levels that authorize them to view the profiles of patrons regardless of whether or not they are in the club on a particular night and to write notes on any patron's profile. WCC has also stated that it only allows necessary employee access to the system. For example, a server would not have access but door staff would.

[40] The software has multiple layers of access control that ensures the WCC has no access to the raw data and the programming of the software. The software also does not allow WCC to print, copy, or in any way extract information from the database without the assistance of TreoScope.

[41] The software is protected with 256 bit encryption. Should the encryption be broken, as an additional layer of security, the information is stored in separate and unidentifiable tables that cannot be reconciled without a specific key (or map) that is stored offsite from the computer at the WCC.

[42] With respect to physical security, it should be noted that at the time of the site visit on April 20, 2007, there was no physical security for the system except for the locked doors of the WCC. This deficiency was brought to Greg Bell's

attention and he stated that he would hire a carpenter to construct an enclosure so that the system was under lock and key. Greg Bell confirmed to the OIPC on August 21, 2007 that the computer that records all of the personal information remains on site but is now in a locked metal cage.

13.0 AUDIT OF WCC INCIDENT RECORDS

[43] The WCC has for many years kept a hand written logbook of any incidents that take place on their property on the days the business is open. The incident log keeps record of which employees were on shift that night, whether or not there where any incidents and details of each incident. It may also include notes on how busy the bar was and whether the police visited the premises. During the site visit we asked to see the handwritten incident log covering the period of the complaint but that log book was not immediately accessible. Mr. Bell agreed to provide select photocopies from the incident logbook of the twelve consecutive months of records beginning six months prior to the installation of the Vigilance software to 6 months after the installation. Records received from the WCC included only dates from January 31st 2004 until December 23rd, 2004 so only records from February 10 until November 10 were used for the audit (*i.e.* a total of ten months of records). The exact date of the Vigilance software installation is unknown. The complainant says the system was in place on June 12, 2004 and the WCC states that it installed the system sometime in June 2004.

[44] The intent of the audit of these records was to determine if there was any correlative evidence of the perceived drop in incidents at the club since the installation of the Vigilance compared to before the installation. An entry in the log was counted as an incident if either a person was removed from the WCC after being admitted or they were involved in an altercation in the WCC parking lot after exiting the WCC.

[45] A review of the incident log revealed that, from February 10, 2004, until June 10, 2004, (I arbitrarily chose June 10, 2004 as the implementation date for the purposes of this audit) there were 13 recorded incidents at the WCC. From June 11, 2004, until November 10, 2004, there were 50 incidents. The WCC stated that the logs and how accurate, up-to-date or detailed they were detailed depended largely on the author at the time which frequently changed because of staff turnover. The WCC believes that the introduction of the system compelled its staff to be more detailed and thorough when completing the written incident log. Records of incidents would now have to be kept in two places (*i.e.* the log book and the system) which allowed WCC management to better audit its door staff and, consequently, produced more complete incident log book entries.

[46] It is also noteworthy that, after the Vigilance software was installed, two people were refused entry that had previously been banned from the WCC while

another patron managed to sneak back into the club after being removed that same night. One other patron, who did not have ID, was found in the club by police and was later noted to be well known to WCC employees and thought to be of age. The WCC contends that the system's effectiveness increases as the size of the database increases.

14.0 RECENT CHANGES TO THE SYSTEM

[47] As of August 20, 2007, TreoScope introduced a new version of its Vigilance Software, version 2.0. This new version, EnterSafe Gateway Security, includes changes to what patron personal information is visible to the WCC and for how long that information will continue to be visible to the business. The same data elements continue to be collected by the software but now less information is visible to the user at the WCC. Now only a patron's name, calculated age and digital photograph are visible to the WCC. Previously, a patron's date of birth, driver's licence number and gender were visible, now these fields can only be accessed via a warrant.

[48] Changes have also been made to the length of time scanned information and notes typed into the system by the user can be viewed by the WCC.

[49] Under the new system, if a patron enters the WCC and there is no recorded "incident" during their visit and they do not revisit within the next six months, then their information becomes inaccessible to the WCC. It remains on the database but will only be retrieved by TreoScope if there is a warrant for the information. If a patron reenters within six months then the clock is reset and their information is visible to the WCC for another 6 months.

[50] If a patron enters the WCC and is involved in an "incident", the WCC may choose to write an internal report about that patron which may be visible to the WCC, at the discretion of Greg Bell, from a minimum of seven days to a maximum of one year (TreoScope states that it is developing a severity level index that will assist businesses in determining what types of incidents warrant different severity ratings but the index is not yet complete). If there are no further occurrences within the one year period, then that information becomes inaccessible to the WCC but is still stored for two years on the database and is accessible via a warrant. However, if another internal report is written within the one year then the original report will be visible until the expiry date of the new report. Also, if a second report is written about a person after one year but before the two year anniversary date then the first report will be visible to the WCC until the expiry date of the second report or until the two year anniversary date, whichever comes first. All report information about a person is deleted from the database two years from its creation.

[51] These same conditions apply to “alerts” that may be inputted into the system if the business wants other establishments to have access to the information. The information placed in an alert would only be available to another business if the patron involved in the incident sought entry to another establishment and had their ID scanned there. As previously noted, the WCC is currently not connected to the internet so this information sharing capability does not apply to it.

[52] TreoScope, in an attempt to help maintain the integrity of notes entered into the system concerning patrons, has added a "disclaimer" screen which requires the user to "accept" or "decline" responsibility for the information they write and the accuracy of that information. TreoScope has also added an advanced audit trail that allows it to track all access movements by a user in the user interface should an allegation of misuse need to be investigated.

NOTICE

Entering The Wild Coyote is considered permission to swipe your I.D. and take your picture. This is for security and identification purposes only. Your information will not be shared or used for marketing purposes. Refusal to produce proper I.D. may result in denied entry.

RECEIVED TIME AUG. 22. 1:37PM

ENTRANCE POLICY

All visitors are required to have one piece of government-issued identification that includes: name, photo, birth date, and signature. (For example: Driver's License or Passport). We are required by law to ask ANYONE who **appears under the age of 25** for two pieces of identification. The second ID must include: name imprinted on card, and photo or signature (for example: Care Card or Social Insurance Card).

Security Screening

All visitors and their personal effects may be subject to search by hand, and, or by metal detectors.

Video Surveillance

These premises are under 24 hour video surveillance. In the event of a criminal or other event in the premises, the video footage will be used to assist the police or other investigation.

ID Scanning

In the event of a criminal or other event in the premises, a police or other investigation may be required. To assist in such an investigation, this establishment wishes to collect and store the following personal information on a TreoScope ID Scanning Station for up to two years: Name; Driver's License Number; Expiry Date; Birth Date; and Gender. Your address will not be collected or stored and none of your information will be used for direct marketing purposes.

Should an incident occur in which an investigation or communication of your information be required, this establishment may use or disclose your personal information to the police, other establishments, or the investigating body and you may be contacted as a potential suspect, witness or other relevant source of information in an investigation.

This establishment reserves the right to deny access to any individual to their premises. Having two pieces of identification does not guarantee entry. If we have any doubts about your ID, you will not be allowed in. If you have legitimate concerns about having your information collected, communicated, and stored by this establishment, please ask to speak to a manager or this establishments privacy officer for alternative options to gain access. Please note: Inspections for compliance are conducted regularly by the Vancouver Police Department and the Liquor Control and Licensing Branch.

TREOSCOPE BARWATCH

ID SCANNING PRIVACY POLICY

Vigilance Software by TreoScope Technologies, Inc.

Vigilance Software and this establishment are committed to protecting the environment within this establishment, the individuals who patron it, and the information necessary for safeguarding it. As providing this service involves the collection, use and disclosure of some personal information about our patrons, protecting their personal information is one of our highest priorities.

In the event of a criminal or other event in the premises, a police or other investigation may be required. To assist in such an investigation, this establishment wishes to collect and store the following personal information on a TreoScope ID Scanning Station for up to two years: Name; Government ID Number; Expiry Date; Birth Date; Gender and Live Photo. Your address will not be collected or stored and none of your information will be used for direct marketing purposes.

Should an incident occur in which an investigation or communication of your information be required, this establishment may use or disclose your personal information to the police, other establishments, or the investigating body and you may be contacted as a potential suspect, witness or other relevant source of information in an investigation.

If you have legitimate concerns about having your information collected, communicated, and stored by this establishment, please ask to speak to a manager or this establishments privacy officer for alternative options to gain access.

TREOSCOPE™

security & data management systems

privacy@treoscope.com

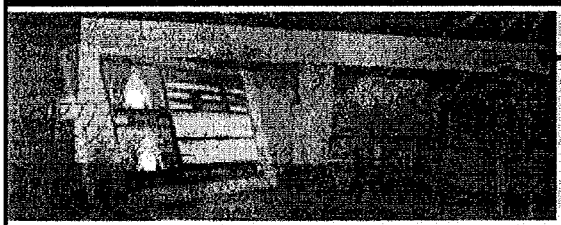
Contact Information for this Establishments Privacy Officer

Name: _____

Mailing Address: _____

_____

Email: _____



TreoScope Technologies, Inc.

TreoScope utilized industry knowledge networks in order to produce an extensive and effective solution set that caters to any operator's needs.

Vigilance Software

VelvetRope Connectivity

Third Party Hardware

Products & Services

TreoScope™ utilized industry knowledge networks in order to produce an extensive and effective solution set that caters to any operator's needs.

TreoScope™ takes pride in being able to quote each individual customer with a turnkey solution that will meet the needs of each specific establishment. Your custom solution will be professionally installed and ready to go in minutes. Always VelvetRope™ ready, TreoScope™ systems running Vigilance Software™ can connect you to the world and bring important security information to your fingertips.

TreoScope™ prides itself on providing a safe and secure method of data management, thus ensuring that the public's information remain protected, while also allowing for an increased amount of security and communication.

Vigilance Software
- > Overview
- > User Interface
- > Verification
- > Due Diligence
- > Client Management
- > Communication
- > Safety
- > FAQ

VelvetRope Connectivity
- > Overview
- > VelvetRope Reports
- > Multiple Locations
- > MarketAware Stats
- > Database Backup
- > Secure Transmission
- > FAQ

Third Party Hardware
- > Overview
- > Components
- > Tech Support
- > FAQ

TREO SCOPE
security & data management systems

Vigilance Software™ acts as a 24/7 doorperson

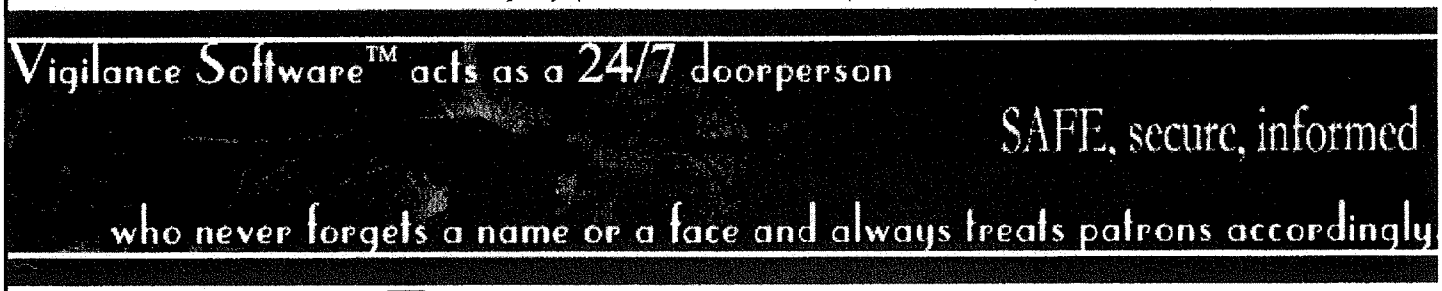
SAFE, secure, informed

who never forgets a name or a face and always treats patrons accordingly

Responsible Host

TreoScope's Vigilance Software™ acts as a 24/7 door person who never forgets a name or a face and always treats patrons accordingly. Establishments are offered both a real and visual deterrent to individuals who could otherwise cause problems. The software pairs a live photo with the information contained on a person's identification, creating a portfolio on each patron requesting entrance. In a fraction of a second, Vigilance Software™ will run a series of queries on the patron requesting entry. By verifying the age and authenticity of the patron's identification, your establishment can stop minors from gaining access and flag trouble makers for your security staff, as well as other establishments subscribed to VelvetRope™. Your VIPs are treated like VIPs while offenders, people under the legal drinking age, and those with fake or tampered-with identifications are turned away.

TREO SCOPE
security & data management systems

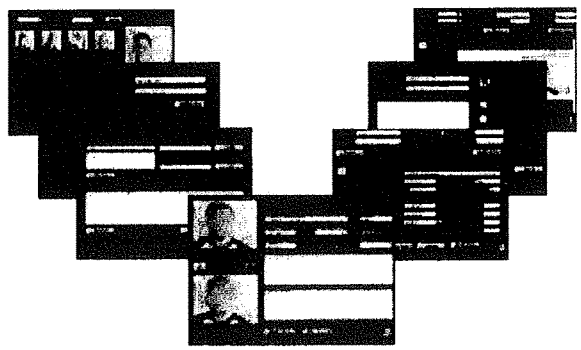


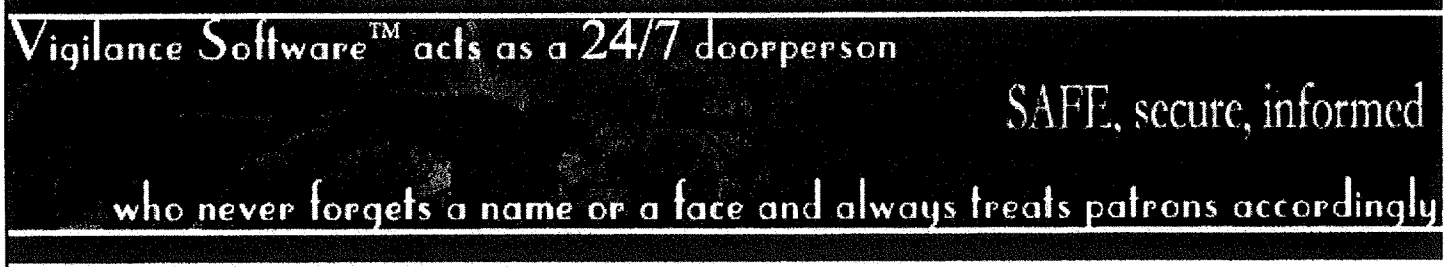
Vigilance Software Product Brochure

Simple, Yet Robust User Interface

Vigilance Software™ is designed to have a simplistic user interface, while housing an extremely swift and robust system beneath. In under a second, a live photo is captured and the patron's information is saved in the system*. Additional information pertaining to the patron, shared via VelvetRope™ Connectivity, is also instantly accessible.

* For privacy reasons, TreoScope's Vigilance Software™ does not extract or process a patron's address. Similarly, the system does not record the patron's height, weight, hair or eye color. Only information necessary for establishment security is recorded.





Informed

>> Age Verification

TreoScope's Vigilance Software™ will not only verify that a patron is of legal drinking age, but also calculate the age so that a doorperson can varify that it reasonably matches the person presenting the identification. Should the patron be below the legal age limit, the operator will be informed immediately and a photo of the underage patron will be taken.

>> Multiple Use Notification

TreoScope's Vigilance Software™ will notify establishment security if an identification card has already been used previously in the same night. If desired, the operator may view the photo captured during the previous entry attempt in order to contrast with the current cardholder.

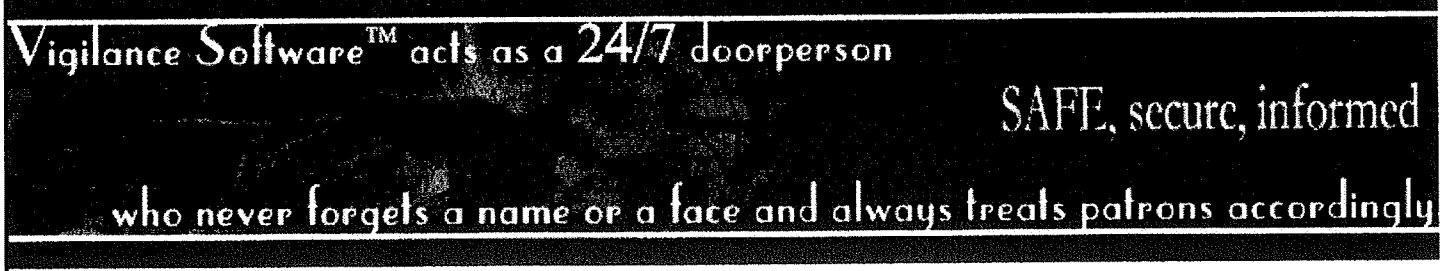
>> Expiry Verification

TreoScope's Vigilance Software™ will verify that a patron's identification card is still valid and hasn't past its expiry date. Should the identification be expired, establishment security will be notified.

>> Authenticity Verification

TreoScope's Vigilance Software™ will recognize all State and Provincial ID's that
comply with the widely accepted government standards for information encoding, and will validate the encoding of each identification card. As such, TreoScope's Vigilance Software™ is an important tool in identifying fraudulent identification. However, security personnel should also verify that the proper security features are present; this includes verifying that the identification card photo matches the individual presenting it.

>> Top



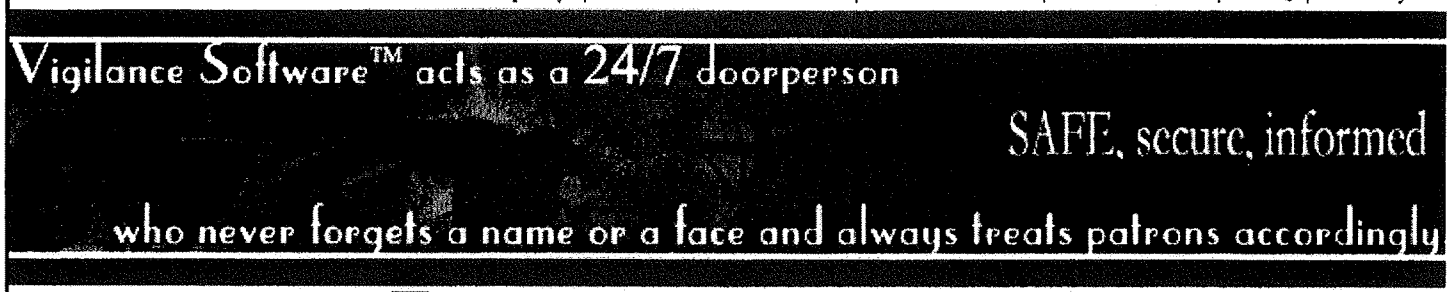
Accountable

>> Identity Fraud

It is important that establishments make every attempt to ensure that minors cannot gain access. TreoScope's Vigilance Software™ will not only verify that a patron is of legal drinking age, but also calculate the age so that establishment security can varify that it reasonably matches the person presenting the identification. Should a minor still gain access to your establishment, through the use of fraudulent identification, establishment security can locate the individual through either a name search or a photo search. This enables establishments to provide law enforcement with proof of due diligence, as well as, holding the minor accountable for identity fraud.

>> Patron Recognition

Responsible operators attempt to create a safe environment for their patrons; however, despite their best efforts incidents will still occur. TreoScope's Vigilance Software™ logs information about all of the patrons attempting entry at an establishment on a given night. Should a problem arise, establishment security can locate the individual(s) through either a name search or a photo search and provide law enforcement with the identites of patrons involved in the incident.



Detailed Client Management

In seconds, an establishment can look up a patron and retrieve any of the internal information on their account. Advanced queries allow management to search and identify patrons in a number of categories, while changing the status of a patron or adding an internal note to their account is merely a click of button.

>> Patron Recognition

TreoScope's Vigilance Software™ logs information about all of the patrons attempting entry at an establishment on a given night. Should the establishment wish to locate an individual who patroned their venue, they can do so by either performing a detailed search based on the patron's account profile, or by performing a patron photo search.

>> Advanced Queries

TreoScope's Vigilance Software™ offers a series of searching tools to help establishments identify their clientele. Using these tools, security personal will be able to identify any patron who has visited that establishment, in a timely fashion.

>> Patron Management

After locating a patron's account, TreoScope's Vigilance Software™ offers the ability to attach an account status to the patron's account. Statuses can be anything from banned to VIP, and are fully configurable by a manager at the respective establishment. In addition, there is also the option to attach an internal note or broadcast a VelvetRope™ Report to a patron's account. Internal notes and statuses apply on an establishment-to-establishment basis, while system wide reports are available to everyone subscribed to VelvetRope™ Connectivity. Should a patron's account status be set to banned, or an internal note or system wide report created, security will be provided with this information the next time the patron attempts entry.

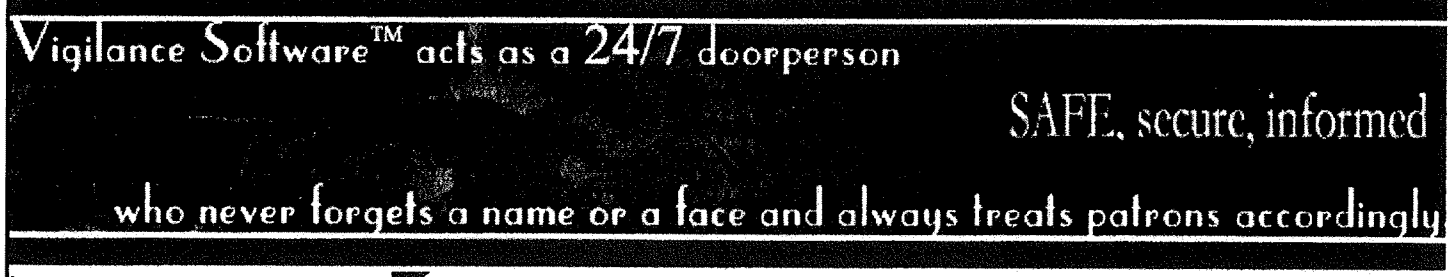
Internal notes can contain any information the establishment wishes to convey to its security about the patron. Good customers can be rewarded, while problem clients will be identified.

>> Patron History

TreoScope's Vigilance Software™ offers establishments the ability to profile a patron's visit history, including the ability to view recent entry photos, total visits, recent visits (within 30days), as well as both internal and VelvetRope™ Reports. This feature serves as a powerful tool in preventing identity theft.

>> Top

TREO SCOPE
security & data management systems



Connected

Always VelvetRope™ ready, TreoScope's Vigilance Software™ can connect you to the world and bring important security information to your fingertips.

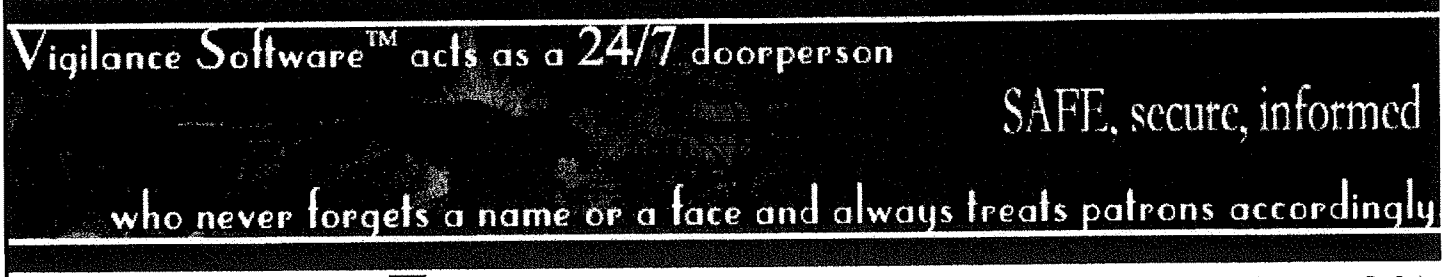
>> External VelvetRope™ Reports

Operators will have the ability to create informative reports on patrons that engage in inappropriate behaviour or activities that endanger other clientele. These reports are broadcasted to all establishments that choose to subscribe to VelvetRope™ Monitoring. Should a patron have a report, the establishment need only click a button to see what it is in regards to, and then handle that patron accordingly.

>> Multiple Location Sharing

TreoScope's Vigilance Software™ caters to establishments that have multiple (local or geographically dispersed) locations. VelvetRope™ Connectivity provides the ability for such establishments to share their patron's internal account statuses and create account notes that will be shared by all locations.

>> Learn more about VelvetRope™ Connectivity



Protected

TreoScope's Vigilance Software™ was designed to protect the environment within an establishment, the individuals who patron it, and the information necessary for safeguarding it.

>> Proactive

Operators utilizing TreoScope's Vigilance Software™ will present both a visual and real deterrent to individuals who may have otherwise caused an incident. Though this software will not stop all problems from occuring in an establishment, it is a valuable security tool that removes anonymity from potential troublemakers, individuals intending to drink-tamper, and patrons visiting from outside the area.

>> Reactive

TreoScope's Vigilance Software™ offers the due diligence necessary to inform law enforcement of the identies of individuals who have caused an incident. Establishment security can also provide proof that they attempted to verify a patron's age prior to admitting them.

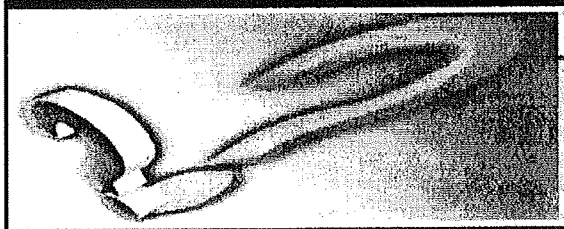
>> Secure

TreoScope's Vigilance Software™ runs on dedicated stations that are fully locked down to prevent any unauthorized access to system data. The software also provides various account privilege levels, which define what a specific operator can use the system for. In addition, all access is tracked and recorded under the identified users account.

The only private information the software extracts is a patrons name, drivers licence number and date of birth. Only authorized governmental agencies have access to information connected to an individual's drivers licence number. No identifiable portion of an address is extracted from an Id, and the user interface offers no ability for an establishment to view the height, weight, hair ,or eye color of a patron. An individual gives more private information when using a credit card or

check then vigilance software extracts from their identification.

>> Top



TreoScope Technologies, Inc.

At TreoScope we strive to deepen public and consumer trust through pulic transparency about our products, and openness and honesty about everything we do.

Frequently Asked Questions

Vigilance Software™

1. What information does the system take from an ID?
2. Why does the software take a live picture of the patron?
3. Does the software have access to a patron's health, driving or criminal records?
4. What identification is the software capable of reading?
5. How long does the system store a patron's information?
6. Can places using this software send mail or email to their patrons?
7. Does the system eliminate the need for security staff to look at a patrons identification?
8. Will the software slow down line-ups?
9. How does the system help prevent minors from gaining access to an establishment?
10. What if a minor gains access to an establishment by using a real identification that is not their own, but the photo bears a considerable likeness to them?
11. What information can establishment view about one of their patrons?
12. Can an establishment add additional information to a patron's account?
13. What if an individual doesn't want to have their ID swiped?
14. What measures are in place to protect the information?

>> What information does the system take from an ID?
TreoScope's Vigilance Software™ extracts a patron's birth date, gender, expiry date, name and driver' licence number.

>> Why does the software take a live picture of the patron?
It is essential that an establishment be able to identify a patron in the system, as such TreoScope's Vigilance Software™ pairs a live photo with the information extracted from the identification. It is important to have a live photo as many embedded identification photos are worn and out-of-date and are little help in identifying a patron. Also, a patron's clothing is an important visual indicator for security staff that have to see so many faces in a given night.

>> Does the software have access to a patron's health, driving or criminal records?
No. The software can only extract information that is already visible on the identification. And, of that information, TreoScope only extracts the information that is absolutely necessary for security purposes.

>> What identification is the software capable of reading?
TreoScope's Vigilance Software™ will only recognize government issued IDs, such as a driver liscence, or state/provincial identification card. It currently supports all such encoded cards issued in North America.

>> How long does the system store a patron's information?
The system stores a patrons information for up to two years as required by law.

>> Can places using this software send mail or email to their patrons?
No. TreoScope's Vigilance Software™ doesn't extract any identifiable portion of an address from the identification. Also, no where on a person's identification is their email address encoded, as such the only way for an establishment to gain access to such information is through alternative means. Under the privacy act, establishments must gain opt-in consent from patrons before collecting and utilizing email or mail information. TreoScope's software is not designed to handle either marketing outlet.

>> Does the system eliminate the need for security staff to look at a patrons identification?
No. TreoScope's Vigilance Software™ is only a tool to be used in addition to normal security procedures. It is important for security to verify the authenticity of an identification's security features, as well as ensure that the user of the ID matches the photo embedded in it.

>> Will the software slow down line-ups?
No. In fact, if TreoScope's Vigilance Software™ is used properly, it

should speed-up the time it takes to move through a line-up. The system takes under a half-a-second to run its queries on an identification and search the database for an account. To ensure the process is a quick one, establishments are urged to make sure that their patron's have their identification out and ready to be swiped.

>> How does the system help prevent minors from gaining access to an establishment?

In addition to calculating a patron's age, Vigilance Software™ verifies the expiry date and authenticity of the identification. Should an identification be used more then once in a given night a multiple use notification will alert the establishment's security personnel.

>> What if a minor gains access to an establishment by using a real identification that is not their own, but the photo bears a considerable likeness to them?

TreoScope's Vigilance Software™ only verifies that an identification is authentic in its encoding and that the age and expiry date are valid. Should a person gain entrance through fraudulent means, the software will have logged their live photo with the information they provided to gain entrance, as such the establishment can provide evidence of due-diligence and the individual can be held accountable.

>> What information can establishment view about one of their patrons?

Establishments can see how many recent and total visits a patron has made to their establishment. In addition, the establishment can view any internal or external reports that are attached to the patrons account. Establishments also have access to the patron's internal statuses and most recent photos.

>> Can an establishment add additional information to a patron's account?

Yes. TreoScope's Vigilance Software™ offers establishments the ability to add internal notes to a patron's account. This information is only available to that particular owner and cannot be accessed outside of the system.

>> What if an individual doesn't want to have their ID swiped?

Establishments are urged to listen to a patron's concerns on a case-by-case basis and should they feel the explanation satisfactory offer an alternative method for the individual to gain admittance.

>> What measures are in place to protect the information?

TreoScope's Vigilance Software™ is housed in a locked down station, which allows the operator access only to the user interface. Only authorized individuals can access the administrative functions, and patron accounts in the user interface. All access is tracked and

recorded under the identified users account.

All information is protected by sophisticated encryption methods and cannot be reproduced or accessed outside of the permissions granted by TreoScope Technologies, Inc. Should an establishment wish to print or save information outside of our user interface, a formal request must be sent and logged by TreoScope Technologies, Inc. or in some cases to a third-party committee.

>> Return to Vigilance Software Section
>> Top of Section
>> Top of Page

VelvetRope™ Connectivity

>> What if an owner has more than one establishment, can they share their internal information?

Yes. Through a VelvetRope™ Connectivity subscription, multiple location sharing is available. This will allow an owner to share internal statuses and other internal information amongst the establishments that he or she owns.

>> What activity or behavior would justify a report being broadcasted?

Establishments can broadcast reports on patrons for everything from failure to pay, drink-tampering, verbal threats and abuse, to involvement in a fight. Though, there are few parameters in what an establishment can broadcast a report about, it is important to note that these reports are subject to approval by a third-party oversight committee. All reports are logged with the authors name and the establishment for which they work.

>> What action should an establishment take if a patron has one or more external reports?

TreoScope urges all clients to make an informed decision on a case-by-case basis. VelvetRope™ External Reports offer no course of action and are only meant to keep establishment security better informed.

>> How many reports can a patron have?

There is no limit to the number of VelvetRope™ External Reports that a patron's account may have. Should a patron have an extensive number of reports detailing violent or dangerous behavior broadcasted recently - then the establishment may notice a clear pattern emerging behind this individual's behavior. Reports are kept on a patron's account for two years as required by law, after which, they are removed from the system.

>> Who can write an external report?

Only authorized owners and managers may use the VelvetRope™ Reporting feature. Access to the feature is password and account restricted and any reports that are broadcasted will contain the author and establishment name.

>> What if a patron feels a report has been unfairly broadcasted?

A patron's first recourse would be to contact the establishment which broadcasted the report. Should dealing directly with the establishment not work, TreoScope's VelvetRope™ Connectivity package also allows for a city or collection of bars to authorize a third-party oversight committee to monitor and approve reports and information requests. Should a dispute arise or a review of an establishment's actions be necessary, the third-party committee would have access to remove reports and mediate between the interested parties.

>> Can an establishment get statistical data from their database?

Yes. VelvetRope™ Connectivity subscribers can choose to purchase MarketAware™ Statistical Reports. However, no personal or private information is revealed in these reports and the information is meant to aid an establishment in targeting its preferred clientele through on-site marketing and promotional activities.

>> What measures are in place to ensure the security of the information being transmitted?

All data is protected using the strongest industry strength encryption algorithms available, which provide up to 256-bit encryption. To compliment this, the network is equipped with a highly sophisticated, multi-level security scheme designed by the engineers at TreoScope™ specifically for VelvetRope™ Connectivity.

>> Return to VelvetRope Connectivity Section
>> Top of Section
>> Top of Page

Third Party Hardware

1. What if an establishment's system gets damaged and the information is lost?
2. Can an establishment use their own hardware components?
3. Can the software utilize an existing surveillance system?
4. If a hardware component fails or an establishment needs technical support with third-party equipment what should they do?

>> What if an establishment's system gets damaged and the information is lost?

Establishments that choose to subscribe to VelvetRope™ Connectivity can be confident that their information is safely and securely backed-up. Should an incident occur that causes an establishments hardware to fail or be destroyed, the operator need only call TreoScope Technologies and request the replacement equipment and have Tech Support restore the database.

>> Can an establishment use their own hardware components?

Establishments may choose to purchase certain hardware components on their own; however, it is recommended that all purchases first be approved by TreoScope™ as compatible with the software.

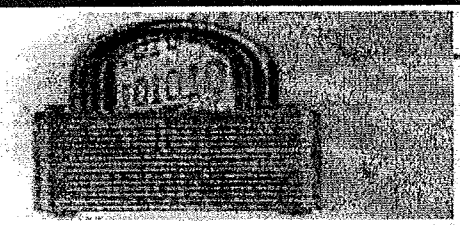
>> Can the software utilize an existing surveillance system?

No. TreoScope's Vigilance Software™ is a self-contained, stand-alone system. It does not currently interact with other software or surveillance systems.

>> If a hardware component fails or an establishment needs technical support with third-party equipment what should they do?

All third party hardware is governed by the warranties and agreements from the original vendor. Should a technical support problem arise with the hardware, please contact the vendor directly. TreoScope will do its best to help customers find prompt and satisfactory solutions to any problems or concerns that may arise from third party hardware.

>> Return to Third Party Hardware Section
>> Top of Section
>> Top of Page



TreoScope Technologies, Inc.

TreoScope's Vigilance Software was designed to protect the environment within an establishment, the individuals who patron it, and the information necessary for safeguarding it.

Privacy

TreoScope's Vigilance Software™ was designed to protect the environment within an establishment, the individuals who patron it, and the information necessary for safeguarding it.

>> Information Extracted

The only private information the software extracts is a patrons name and drivers licence number. Only authorized governmental agencies have access to information connected to an individual's drivers licence number. No identifiable portion of an address is extracted from an Id, and the user interface offers no ability for an establishment to view the height, weight, hair ,or eye color of a patron. An individual gives more private information when using a credit card or check then vigilance software extracts from their identification.

TreoScope Technologies, Inc. has no access to a persons driving record, medical history, or criminal records. Only information visually contained on the licence can be accessed by the software, and of that, only necessary information for the maintenance of a safe environment is extracted.

>> Top

>> Information Shared

TreoScope's VelvetRope™ Connectivity allows establishments to transmit external reports of alleged offenders to one another. These reports contain the name of the individual involved, a description of the incident, a photo of the individual taken from the night in question, and the date of the alleged incident. Also attached is the name of the establishment broadcasting the report, their phone number, and the name of the person who wrote the report.

A persons height, weight, eye color, hair color and the drivers licence number is not visible in an external report. Reports cannot be printed without a logged request being sent to either TreoScope Technologies, Inc. or in some cases to a third-party committee.

>> Top

>> Third-Party Oversight Committee

TreoScope's VelvetRope™ Connectivity package allows a city or collection of bars to authorize a third-party oversight committee to monitor and approve reports and information requests. This feature ensures that an establishment cannot launch a report without it first being authorized by a neutral panel and all information requests will also be viewable by the committee. Should a dispute arise or a review of an establishment's actions be necessary, the third-party committee would have access to remove reports and mediate between the interested parties.

>> Top

>> Information Safeguarded

TreoScope's Vigilance Software™ is housed in a locked down station, which allows the operator access only to the user interface. Only authorized individuals can access the administrative functions, and patron accounts in the user interface. All access is tracked and recorded under the identified users account.

All information is protected by sophisticated encryption methods and cannot be reproduced or accessed outside of the permissions granted by TreoScope Technologies, Inc. Should an establishment wish to print or save information outside of our user interface, a formal request must be sent and logged by TreoScope Technologies, Inc. or in some cases to a third-party committee.

>> Top

>> Law Enforcement

Law enforcement agencies may from time to time need information stored and, or contained in our clients databases - such requests must be made to the establishment in question and must also have a court order, warrant, and or subpoena for the requested information.

>> Top

>> Information Stored

TreoScope's databases maintain only the necessary and relevant information on a patron. This information is kept current with every visit to a particular establishment. Information remains safeguarded within our databases for a period up to two years - as necessary by law.

>> Contact Privacy

>> Top

PRIVACY POLICY

Vigilance Software by TreoScope Technologies Inc

Vigilance Software and this establishment are committed to protecting the environment within this establishment, the individuals who patron it, and the information necessary for safeguarding it. As providing this service involves the collection, use and disclosure of some personal information about our patrons, protecting their personal information is one of our highest priorities.

Basic Definitions

Personal Information

- Means information about an identifiable individual
- Vigilance Software is equipped to record the following *Personal Information*:
    1. Driver's Licence number
    2. Full Name
    3. Date of Birth
    4. Expiry Date
    5. Gender
    6. Live photo of the individual
- Vigilance Software does **not** record an individual's address

NOTE: Vigilance Software Version 2.0 will record the Date of Birth, but will only make the calculated age visible to the establishment. The DOB will only be made available when required by law.

Contact Information

- Means information that would enable an individual to be contacted at a place of business.
- Vigilance Software does not offer establishments any *Contact Information* and is; therefore, not covered by this policy

Privacy Officer

- Means the individual designated responsibility for ensuring that this establishment complies with this policy
- The *Privacy Officer* should be made available to answer any questions or concerns the public may have about this establishments' use of Vigilance Software.

Policy 1 – Collecting Personal Information

1.1 Communicating the purposes for collection

- This establishment will post signage indicating the purposes for which personal information is being collected, before and at the place of collection into Vigilance Software.

1.2 Purposes for which personal information will be used

- This establishment and Vigilance Software will only collect *Personal Information* necessary to fulfill the following purposes:
    1. To verify that the individual is of the legally permitted age to gain entry
        - Vigilance Software records an individual's *Date of Birth* to calculate the age

- Vigilance Software records an individual's *Expiry Date* to ensure ID is valid

2. To verify the authenticity of the identification being provided
   - Vigilance Software checks a unique parsing sequence to ensure compatibility with the jurisdiction being provided. In addition, identification that may have been visually altered will display the original encoded information
3. To ensure that identification is only used by the entitled individual
   - Vigilance Software uses an individual's *ID Number* to check for past entry into the software, it then recalls the early *Photo* of the individual using the same identification
4. To track the number of visits and familiarity with that individual
   - Vigilance Software uses an individual's *ID Number* to track their number of visits to this establishment. It also allows for this establishment to tie internal statuses and notes to that individual's account
5. To identify individuals who have caused a problem and maintain or communicate a record for later review
   - Vigilance Software uses an individual's *ID Number, Name, Date of Birth* and *Photo*
6. To assist in an investigation, legal or business dispute
   - Vigilance Software uses an individual's *ID Number, Name, Date of Birth* and *Photo*
7. To ensure a high standard of safety and service to our patrons

Policy 2 – Consent

2.1 Obtaining Consent

➔ This establishment will obtain an individual's consent to collect, use or disclose personal information (except where, as noted below, we are authorized to do so without consent)

2.2 Implied Consent

➔ This establishment will consider the consent is implied as the purpose for collection is considered obvious (as well as disclosed in signage)

➔ Due to this establishments commitment to ensuring that Vigilance Software be made visible to the individuals prior to their entry into the system, as well as being openly disclosed in signage, we will consider the consent is implied as the individual is given a reasonable opportunity to ask questions or raise an objection prior to been entered into the system,

➔ This establishment will consider the consent is implied as the individual will voluntarily provide their personal information (by handing over their identification at the Vigilance Software check point) for entry into Vigilance Software.

2.3 Implied Consent through Notice

➔ It is this establishment's policy, that if an individual has not raised a concern or attempted to opt-out after reading our signage, visually seeing Vigilance Software in use, and handing over their identification for scanning into the software, then the consent is implied.

2.4 Withhold or Withdraw Consent

- It is this establishment's policy, that in order to provide the safe, age-restricted environment and service that is required by law, then the collection, use or disclosure of *Personal Information* recorded into Vigilance Software is permitted and a decision by an individual to withhold or withdraw consent will restrict our ability to provide that service and may potentially frustrate the performance of our legal obligation.
- However, subject to certain exceptions (review of an individual's identification is required by law), this establishment may provide individual's with an alternative method of entry at the sole discretion of management.

NOTE: Vigilance Software allows this establishment to comply with the Liquor-Primary License – Terms & Conditions suggestion to "record each person's name and ID serial number… [and] use video surveillance to record an image of the person and his or her ID."

2.5 Collection, Use or Disclosure of Personal Information Without Consent

- This establishment may collect, use or disclose *Personal Information* without the individual's knowledge or consent in the following limited circumstances:

1. When the collection, use or disclosure of personal information is permitted or required by law;
2. In an emergency that threatens an individual's life, health, or personal security;
3. When we require legal advice from a lawyer;
4. To protect ourselves from fraud;
5. To investigate an anticipated breach of an agreement or a contravention of law

Policy 3 – Using and Disclosing Personal Information

3.1 Disclosing Personal Information

- This establishment only use or disclose an individual's *Personal Information* where necessary to fulfill the purposes identified at the time of collection.

3.2 Additional Purpose for Disclosing Personal Information

- This establishment will not use or disclose an individual's *Personal Information* for any additional purpose unless we obtain consent to do so.

3.3 Selling Personal Information

- This establishment will not sell customer lists or *Personal Information* to other parties unless we have consent to do so.

Policy 4 – Retaining Personal Information

4.1 Personal Information with added Notes, Statuses or Records

- If this establishment uses an individual's *Personal Information* to make a decision that directly affects the client – such as an internal note, status change, or report – we will retain that

Personal Information for two years so that the individual has a reasonable opportunity to request access to it.

4.2 Personal Information without added Information

- Subject to policy 4.1, we will retain an individual's *Personal Information* for a period of two years to fulfill the identified purposes or a legal or business purpose.

NOTE: Vigilance Software Version 2.0 has made the following changes to the Retention Policy within the software:

4.1 Personal Information with Added Notes or Statuses

- If this establishment uses an individual's *Personal Information* to make a decision that directly affects the client – such as an internal note or status change – we will retain that *Personal Information* for at least one year, from the last date of entry into the establishment, so that the individual has a reasonable opportunity to request access to it.
- If this establishment uses an individual's *Personal Information* to make a decision that directly affects the client for a specified period of time, we will retain that *Personal Information* for at least one year from its expiry so that the individual has a reasonable opportunity to request access to it. Expired information will be hidden and inaccessible from the establishment and stored safely in a backend database until the date of its deletion.

4.2 Personal Information Used to Produce a Report

- If this establishment uses an individual's *Personal Information* to produce a report that directly affects the individual, we will retain that *Personal Information* for at least one year from its expiry so that the individual has a reasonable opportunity to request access to it. Expired information will be hidden and inaccessible from the establishment and stored safely in a backend database until the date of its deletion.
- Should this establishment write a report using Vigilance Software; the report will be visible to the establishment for the preset time period that corresponds with the severity level of that report. Once that report expires it will become hidden and inaccessible from the establishment and stored safely in a backend database until the date of its deletion.
- However, should another report be written about an individual before their previous report has been deleted, both will be visible for the most recent report's severity time period and both reports will now be reset to delete at least one year after the most recent report expires, so that the individual has a reasonable opportunity to request access to it.

4.3 Personal Information without added Information

- Subject to policy 4.1 and policy 4.2, we will retain an individual's *Personal Information* for a period of six months from the last date of entry into the establishment to fulfill the identified purposes or a legal or business purpose.

Policy 5 – Ensuring Accuracy of Personal Information

5.1 Ensuring Accuracy of Personal Information

- This establishment has chosen to utilize Vigilance Software, which allows it to read government issued identification. The information extracted from the identification is processed directly by Vigilance Software and offers the establishment no ability to alter or complete the *Personal Information* contained on the ID.
- Vigilance Software does **not** allow the establishment to alter or complete the *Personal Information* of an individual, as the information is being provided by a government agency and its accuracy is assumed and legally required.
- Should an individual's information be in error, they should immediately be instructed to advise the issuing government agency to update their identification and records.

5.2 Requests to Correct Personal Information

- This establishment has no ability to correct the *Personal Information* of an individual stored in Vigilance Software. Corrections to the *Personal Information* of an individual can only be made with updated government identification.

5.3 Annotating Correction Requests to Personal Information

- This establishment will make an internal note against an individual's account should it be demonstrated that their *Personal Information* is inaccurate or incomplete. Though a formal correction cannot be made within the software, a correction request will be noted in their file.

Policy 6 – Securing Personal Information

6.1 Ensuring Security of Personal Information

- This establishment in partnership with Vigilance Software is committed to ensuring the security of an individual's *Personal Information* in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

6.2 Security Measures in use to Protect Personal Information

- This establishment in partnership with Vigilance Software will enforce the following security measures to ensure that c an individual's *Personal Information* is appropriately protected:

1. This establishment will physically store the Vigilance Software Scanning Station in a safe, access restricted environment;
2. This establishment will utilize Vigilance Software's access levels and user logins to ensure that only the appropriate employees have access to the areas of the software deemed necessary;
3. This establishment will only grant user access to individuals who need such access;
4. Vigilance Software ensures that this establishment has no access to the backend databases and software, and as such, this establishment may only use the software for the intended purposes;
5. Vigilance Software does **not** allow this establishment to print, copy, or in any way extract information from the database without first presenting a reason set forth in Policy 2.5.

6. Vigilance Software is protected by multiple layers of 256 bit encryption
7. Vigilance Software has multiple layers of access control into the backend and database
8. Vigilance Software's database stores information in separate and unidentifiable tables that cannot be reconciled without a key stored offsite from the field unit.
9. Any communication between Vigilance Software and TreoScope Technologies (the software and database maintenance company) is zipped, encrypted and sent over a secure port to port authentication procedure.

New Feature in Vigilance Software Version 2.0	10. Vigilance Software has an advanced audit trail, which shows all access movements by a user in the user interface.

6.3 Destroying Personal Information

➔ This establishment in partnership with Vigilance Software will use appropriate security measures when destroying an individual's *Personal Information* such as: shredding documents and deleting electronically stored information.

6.4 Continual Updating of Security Policies and Controls

➔ This establishment in partnership with Vigilance Software will continually review and update our security policies and controls as technology changes to ensure ongoing *Personal Information* security.

Policy 7 – Providing Access to Personal Information

7.1 Access to Personal Information

➔ Individual's have a right to access their *Personal Information* stored in this establishment's Vigilance Software, subject to the following limited exceptions:

1. The information is protected by solicitor-client privilege;
2. The information was collected or disclosed without consent, as in policy 2.5, for the purposes of an investigation and the investigation and associated proceedings and appeals have not been completed;

7.2 Written Request to Access Personal Information

➔ A request to access personal information must be made in writing and provide sufficient detail to identify the *Personal Information* being sought. A request to access *Personal Information* should be forwarded to the Privacy Officer.

7.3 Explanation of Use and Disclosure of Personal Information

➔ Upon request, we will also tell an individual how we use their *Personal Information* and to whom it has been disclosed if applicable.

7.4 Time Frame for Access to Personal Information

➔ We will make the requested information available within 30 business days, or provide written notice of an extension where additional time is required to fulfill the request.

7.5 Fee for Access to Personal Information

➔ A minimal fee may be charged for providing access to personal information. Where a fee may apply, we will inform the individual of the cost and request further direction from the individual on whether or not we should proceed with the request.

7.6 Refusing Access to Personal Information

➔ If a request is refused in full or in part, we will notify the individual in writing, providing the reasons for refusal and the recourse available to the individual.

Policy 8 – Questions and Complaints: The Role of the Privacy Officer

8.1 Role of Privacy Officer

➔ The Privacy Officer or designated individual is responsible for ensuring this establishment's compliance with this policy and the governing privacy protection act.

8.2 Complaints, Concerns, or Questions about Compliance

➔ Individuals should direct any complaints, concerns or questions regarding this establishment's compliance in writing to the Privacy Officer. If the Privacy Officer is unable to resolve the concern, the individual may also write to the governing body in charge of enforcing compliance to the privacy protection act.

Contact Information for this Establishment's Privacy Officer

Name: _____

Mailing Address: _____

_____

_____

Telephone: _____

Email: _____

Adoption of the above Privacy Policy

Name of the Establishment: _____

Policy Adoption Date: ____/____/____ dd/mm/yyyy

Authorizing Signature _____

Name of Authorizing Party _____

Title of Authorizing Party: _____

The second piece must:

- include an imprint of the holder's name (e.g. a credit card or Care Card), and
- include the person's signature and/or picture.

If the person cannot produce two pieces of acceptable identification that proves they are 19 or older, you must refuse entry.

You must cooperate with a liquor inspector if the inspector asks you or your staff to determine whether a person is a minor.

To verify identification, ask the person for:

- A sample signature to compare to the signature on the photo identification.
- His or her zodiac sign – people with false identification often will be unable to answer quickly.
- His or her middle name and how to spell it.
- Information that is on the identification, such as the person's address or postal code.

You are encouraged (but not required) to retain identification that is clearly false and to turn it over to your liquor inspector. Where possible, the inspector will return the identification to the agency that issued it. (If the patron insists you return the ID, you should do so, but we encourage you take a photocopy of it first to give to your liquor inspector.)

Setting aside an area to check ID

You must provide an area in your establishment that is well lit and protected from entertainment noise so that staff can properly review both the offered identification and the patron, and ask appropriate questions to test the ID's authenticity.

If you operate an establishment that is particularly attractive to young people, you will be expected to maintain a sufficient standard of scrutiny to prevent access by minors. To help deter minors, we suggest you:

- record each person's name and the ID serial number
- assign an experienced doorperson to check ID
- secure any uncontrolled exits, as allowed in fire safety rules, regulations or codes, and
- use video surveillance to record an image of the person and his or her ID.

If your procedures are not effective, your local liquor inspector may direct you to install the appropriate lighting, signage, video cameras and noise barriers to ensure your staff can check identification properly. (Licensees directed to install and operate video cameras may be required to provide the film from those cameras for review by the branch.)

Overcrowding

Your liquor licence tells you the maximum number of patrons or the maximum number of persons (patrons and staff) that you may allow in your premises at one time (see the definitions of "patron capacity" and "person capacity" at the beginning of this guide).

It is important for you to know the type of capacity for which your establishment is licensed, and to make sure you stay within this limit. You must have controls at each entry point to your establishment, and you must be able to count the number of people entering and leaving.

Please note:
If an inspector visits your establishment and is uncertain as to whether it is overcrowded, the inspector will count, as accurately as possible, the number of patrons/persons in your establishment.

If the count indicates that your establishment is overcrowded, the inspector will, if possible, do a second count. If you receive a Contravention Notice (please see the section on Inspections for more on this), it will include both the first and second count.

Local building/fire authorities also establish a maximum capacity or occupant load that may differ from your liquor licence maximum capacity. (In most cases, the occupant load maximum capacity will be greater than the liquor licence maximum capacity.) You may apply to the branch to increase your liquor licence maximum capacity so that it matches the occupant load maximum capacity set by building and/or fire authorities. If fire and building officials have each calculated an occupant load for your establishment, or if an engineer or architect has, and the numbers are not the same, the lower number is the one you must use.

Drink sizes

You must encourage moderate consumption at all times and follow strict limits on the maximum size of servings.

Distilled liquor: Each drink containing distilled liquor (spirits) shall not contain more than three

http://www.pssg.gov.bc.ca/lclb/publications/guides-licensee/LiquorPrimary.pdf