



BY FAX (604) 688-1237

August 20, 2009

Owen Cameron
President
TreoScope Technologies Inc.
Suite 308
21 Water Street
Vancouver BC V6B 1A1

Dear Owen Cameron:

Consultation on driver's licence scanning in bars—Order P09-01—OIPC File P09-38989

This letter, which reflects our discussions with you over the past few weeks respecting TreoScope's EnterSafe system, sets out my views on personal information collection using that system and on associated personal information retention periods.

Background

A number of comments in the media about the impact of Order P09-01 and what it means for customer and public safety do not square at all with the actual decision. It is therefore important to again underscore that, in Order P09-01, I expressly and repeatedly acknowledged that licensed establishments should 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" (paras. 127 and 152).

Based on the material before me in that case, I concluded that much of the information collected by TreoScope's EnterSafe system at the relevant time—including, for example, driver's licence numbers—did not further this safety purpose. I also found that no persuasive reason related to improved customer safety had been provided for a licensed establishment's retention of information relating to customers who are not involved in violent incidents (para. 127). In the end, I found that the collection of personal information as a whole, as it was being conducted at the time of the underlying investigation report, did not comply with PIPA.

Quite understandably, I received no submissions in the inquiry leading to Order P09-01 on how the system would operate if it were aimed at only maintaining a list of banned customers. I therefore strongly encouraged those involved to seek my office's views if they wished to find a solution for collecting personal information of a nature, and in a manner, that complies with PIPA.

Since then, my office has had discussions with you with a view to identifying elements of customer personal information that may be collected, used and disclosed for the customer

safety purpose affirmed by Order P09-01. We have also discussed retention periods in view of s. 35 of PIPA.

You told us that you have discussed these issues, including as to specific personal information elements and retention periods, with TreoScope customers and other stakeholders, including at least one industry association and a representative of at least one police force. We understand they are aware of our discussions with you and that you believe what is set out below is a workable solution in terms of meeting the customer-safety goals acknowledged in Order P09-01.

What follows is certainly the acceptable solution from my perspective. Specifically, it is my view that the collection, use and disclosure of the following elements of personal information, and their retention as addressed below, would comply with PIPA as contemplated by Order P09-01.

Personal information elements to be collected

You have told us that the EnterSafe system will be re-designed and then deployed across all existing and future installations so that it will, moving forward, collect only the following personal information of customers at the point of their admission to a licensed establishment (collectively, excepting the postal code information noted below, "Identifying Information"):

- name;
- date of birth ("DOB");
- photo (taken on the spot, not the photo from the driver's licence or BC ID presented at entry);
- gender; and
- the first three letters of the customer's postal code.

A licensed establishment will have read-only access to the customer's name, photo and calculated age (not DOB). The system will also inform security staff if the piece of identification presented has expired.

TreoScope's servers will retain the Identifying Information. The first three letters of the postal code will also be retained in the system, but these data elements will be dissociated from Identifying Information, *i.e.*, TreoScope will ensure that these data elements are no longer personal information and cannot be reconstituted as such. This non-personal information may, you have told us, be used as part of a TreoScope service to licensed establishments to let them know where their customers are coming from in terms of broad geographic areas of customer origin.

The Identifying Information in my view represents an acceptable reduction in the nature and scope of the personal information to be collected, used and disclosed through the EnterSafe system for customer safety purposes. We understand from you that this Identifying Information will be sufficient to enable identification, using the EnterSafe system, of customers who have been determined to be undesirable for re-entry from a safety perspective.

Retention of personal information

The EnterSafe system will, subject to what is said below, retain the Identifying Information of all customers for only a period of 24 hours after the establishment closes on the day on which the Identifying Information was collected (or the day immediately following, where the establishment closes after midnight). After the 24-hour period, a customer's Identifying Information will be completely and permanently deleted from the EnterSafe system in all places, *i.e.*, both from each establishment's computers and TreoScope's servers. Identifying Information must not be retained in any other medium by anyone, including TreoScope and licensed establishments.

An example will illustrate what is intended by the 24-hour retention period. If a customer's Identifying Information is collected on September 1 at 10:00 PM, but the establishment closes at 3:00 AM on September 2, the customer's Identifying Information will be retained until 3:00 AM on September 3. If the customer's Identifying Information is collected at 2:00 AM on September 2, it will still be retained until 3:00 AM on September 3.

I can understand some might wonder whether the language of s. 35(1) of PIPA could be read to require retention of *all* customers' Identifying Information for at least one year, even where they have not been determined to be undesirable for re-entry. A purposive approach to interpretation of PIPA is required by the *Interpretation Act* and by numerous decisions of the Supreme Court of Canada. This requires me to consider the purposes of PIPA stated in s. 2, the language of s. 35 itself, and the statutory context in which it is found (including the existence in PIPA of the right of access to one's own personal information, the right to request correction of errors and the duty of organizations to make reasonable efforts to ensure personal information is accurate and complete). Taking all of this into account, in my view customer Identifying Information that is provided at the point of admission and does not result in a decision to deny entry does not trigger the one-year minimum retention period in s. 35(1) of PIPA for personal information used to make a decision directly affecting an individual.

By contrast, an establishment will, for more than the 24-hour retention period, retain, use and disclose to other establishments, through EnterSafe, the Identifying Information of a customer who it determines is violent or otherwise undesirable for re-entry from a customer safety perspective. That customer's Identifying Information and other personal information used to make the decision to bar his or her entry must be retained by the establishment for a minimum of one year, regardless of the length of the ban. For example, if a customer is determined to be undesirable for entry and is banned for six months, both the Identifying Information and any other personal information compiled about the customer and used to make the banning decision must be kept for one year after the decision is made. The customer's personal information may be retained for a longer period when necessary—for example, if there is a longer-term ban or it is used in relation to repeated incidents and bans over time.

Preventing minors from entering licensed establishments

At para. 123 of Order P09-01, I acknowledged that, where there is some question about whether a customer is of legal drinking age, it may be reasonable to scan a piece of identification to verify its authenticity and to ensure that the customer is of legal drinking age. Consistent with my finding regarding customer safety, however, I found that much of the information collected by the EnterSafe system at that time did not fulfill the purpose of ensuring that minors do not enter an establishment. I also found that the purpose was not furthered by actually recording the information embedded in the card and retaining it.

Further, in Order P09-01 I indicated that this purpose is not served by the scanning of identification of those individuals who are clearly of legal drinking age. Since the release of Order P09-01, we have had constructive discussions with officials from the Liquor Control and

Licensing Branch of the Ministry of Housing and Social Development about the need to deter minors from entering licensed establishments and the scale of that problem. In view of the fact that, consistent with this letter, the Identifying Information of *all* customers will be collected and retained for at least 24 hours for customer safety purposes, as discussed above, I accept that it is appropriate to collect and use a customer's DOB to calculate her or his age, and display calculated age only at the point of admission, for the purposes of determining that the customer is of legal drinking age. I also acknowledge and accept that the EnterSafe system will, as noted above, indicate if a piece of identification has expired and that it will indicate if it has already been scanned on that same date.

The above discussion about retention periods applies here. The Identifying Information of a customer who is of legal drinking age may not be retained for longer than the above 24-hour period, unless of course that individual is barred from re-entry, as discussed above. Also consistent with the above discussion, the Identifying Information of a customer who is determined to be under age and is thus barred from entry is retained under s. 35(1) and consistent with s. 35(2).

It should be emphasised that the acceptability of collecting Identifying Information of all customers to determine whether they are of drinking age is entirely dependent on the fact that this same information of all customers is in any case being collected for customer-safety purposes and retained for only 24 hours unless a customer is denied entry as discussed above. I withhold comment on whether, in cases where there is no added, valid customer safety purpose that authorizes collection of this same Identifying Information anyway, it is appropriate to collect personal information of individuals who are clearly of legal drinking age for age-verification purposes.

Other issues

For clarity, this letter addresses only which personal information elements may be collected using the EnterSafe system and associated retention issues. It does not mean that my office will not or cannot investigate complaints of breaches of PIPA arising from, for example, an organization's misuse of the EnterSafe system or alleged personal information security failures.

Nor does this letter address other issues dealt with in Order P09-01, notably PIPA's requirement that each organization that collects, discloses and uses customer personal information using the EnterSafe system must:

- provide notice of collection of personal information at the time of collection;
- have policies and procedures for compliance;
- develop a complaint process;
- make information about its policies, procedures and complaint processes available on request;
- appoint a privacy officer who is responsible for compliance.

This letter also does not address compliance issues associated with an organization's obligations to:

- make reasonable efforts to ensure that personal information it collects is accurate and complete where it is likely to be used to make a decision to affect an individual or to be disclosed to another organization;
- respond to an individual's request to correct an error or omission in his or her personal information;
- give an individual access to his or her own personal information where requested by that individual, subject to any applicable exceptions to disclosure;
- make reasonable security arrangements to 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.

I appreciate TreoScope's open and professional approach to finding a workable solution that meets the needs of its customers, and the purposes of customer safety, in a privacy-compliant manner.

Please contact me immediately if you have any concerns about the contents of this letter.

Yours sincerely,

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

Copies: Karen Ayers
Assistant Deputy Minister and General Manager
Liquor Control and Licensing Branch
Ministry of Housing and Social Development

John Teti
Chair, BarWatch Vancouver

Scott Gurney
Victoria Bar & Cabaret Association

Al Arbuthnot
President, ABLE BC

Deputy Chief Constable Steve Sweeney
Vancouver Police Department

Deputy Chief Bill Naughton
Victoria Police Department