



DOLDEN WALLACE FOLICK LLP

Insurance Law Update

Insurance Law Expertise... It's our policy.

May 6, 2011

COMMERCIAL HOSTS' USE OF IDENTIFICATION-CAPTURING TECHNOLOGY CREATES PRIVACY ISSUES



Software designed to scan and store the personal information of bar patrons provides commercial host establishments with an effective screening mechanism to identify members of criminal organizations and problem patrons. Does this technology infringe of privacy rights? In July 2009, the B.C. Privacy Commissioner determined that it did.

The software provides instantaneous ID verification and documentation of any North American driver's license. The software creates a digital profile of patrons by recording their name, photograph, date of birth and ID serial number. Patrons' personal information is sent encrypted over the internet to a database in Vancouver. The personal information can only be accessed if police present a warrant, and the information is purged two years after creation.

Despite positive reviews, privacy concerns have plagued the software. Critics have argued that it is in breach of Canada's *Personal Information Protection Act* ("PIPA"); legislation designed to set the ground rules for how private sector and not-for-profit organizations may collect, use or disclose personal information. Section 2 of the *PIPA*, explicitly recognizes the "right of individuals to protect their personal information..."

The privacy concerns were addressed in the B.C. Privacy Commissioner's decision concerning the use of the software at the Wild Coyote, a Vancouver nightclub.

Following a review of its practices and procedures, the B.C. Privacy Commissioner ordered Wild Coyote to stop scanning IDs, stop collecting patron's personal information and to ensure that any such information in the software's database was destroyed. The Commissioner felt that Wild Coyote was collecting too much information, and storing it for too long.



DOLDEN WALLACE FOLICK LLP

Insurance Law Update

Insurance Law Expertise... It's our policy.

In July 21, 2009, the B.C. Privacy Commissioner ruled that Wild Coyote could not require an individual to consent to the collection, use or disclosure of personal information, through the use of the software, as a condition of supplying a product or service. To do so would violate section 7 of the PIPA:

[7] 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.

The Commissioner found it troubling that, despite repeated assertions that the software has dramatically improved safety and security, no material such as statistics were presented that persuasively demonstrated an actual reduction in violent incidents in the Wild Coyote. There was simply no evidence to support the claim that the collection and storage of the personal information played a significant role in achieving a safe environment.

Based on the foregoing, the Commissioner stated:

[99] ... I find that the collection of customer information through the use of the ... system ... is not "necessary" within the meaning of section 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 ... 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 ... software or through retaining ID during the period of a customer's visit as a condition of supplying a product or service.

The Commissioner further determined that the Wild Coyote's use of the software was in breach of sections 8(1), 10(1), 11, and 23(1) of the PIPA.



DOLDEN WALLACE FOLICK LLP

Insurance Law Update

Insurance Law Expertise... It's our policy.

Following the above decision, the software manufacturer and the Privacy Commissioner agreed in August 2009 to a new protocol which permits the continuation of the software in British Columbia. In essence:

[the software] can now be used to collect only the name, photograph, date of birth and gender of customers who enter a bar, but that information can be retained for no more than a transitory 24-hour working period. After that, customer information is completely destroyed.

However, if a customer is determined within the transitory 24-hour working period to be violent or otherwise undesirable from a safety perspective, that customer's name, photograph, date of birth and gender can be kept, and shared with other bars using [the software] for customer safety purposes.

In 2006, the Office of the Information and Privacy Commissioner of Alberta ruled on a similar issue. The complainant made a complaint under Alberta's *Personal Information Protection Act* that an employee of Tantra Nightclub had scanned his driver's licence information into a data base without his consent.

The Commissioner found that Tantra did not have a reasonable purpose when it collected the complainant's driver's license information. In addition, the Commissioner found that Tantra did not have a reasonable purpose for retaining the driver's license information of patrons.

As a result, the Alberta Commissioner found that the collection of the complainant's personal information, and that of other patrons, was in violation of sections 7, 8, 13 and 14 of the *Act*. The Commissioner found that the organization had not taken reasonable steps to secure the complainant's personal information under section 34, and had contravened section 35 when it retained the complainant's driver's license information. The commissioner held:

[47] ... section 7(2) makes it clear that an individual cannot be required to consent to the collection of information that is unnecessary for the supply of a product or service. In the present case, the organization collected the complainant's driver's license information as a condition of entering Tantra. The organization has not established that collecting all the information on the complainant's driver's license was necessary to complete the transaction.



DOLDEN WALLACE FOLICK LLP

Insurance Law Update

Insurance Law Expertise... It's our policy.

The rulings in B.C. and Alberta demonstrate that the Privacy Commissioners are committed to enforcing the individual's privacy rights. Software must comply with privacy legislation, particularly with regard to the consent, disclosure, storage and use of personal information. This will require organizations developing identification-capturing software to be aware of the privacy legislation, and be prepared to defend their actions when confronted from both patrons at licensed establishments, and privacy watch groups.

AUTHOR: Lorne P.S. Folick

Direct: 604.891.0352

Email: lfolick@dolden.com

CO-AUTHOR: Trevor R. Thomas

Direct: 604.891.0369

Email: tthomas@dolden.com

This newsletter is for general information only and is not intended to provide, and should not be relied on for, legal advice in any particular circumstance or fact situation. Readers are advised to obtain legal advice to address any particular circumstance or fact situation. The opinions expressed in this newsletter, if any, are those of the author and not necessarily of Dolden Wallace Folick LLP or its clients.