# Reviewing the Licensing Automation System of the Ministry of Natural Resources:

# A Special Investigation Report

## Privacy Investigation Report
## PC12-39

June 27, 2012

Information & Privacy Commissioner,
Ontario, Canada

Ann Cavoukian, Ph.D.
Commissioner

# Table of Contents

# Background

On May 16, 2012, during Question Period in the Ontario Legislative Assembly, two members of provincial parliament (MPPs) asked the Minister of Natural Resources questions about the privacy and security of personal information that is currently being stored in the U.S. as part of the Licensing Automation System (LAS) database of the Ministry of Natural Resources (the Ministry). Specifically, the MPPs raised concerns about the collection and storage of personal information as part of the LAS, in light of the U.S. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (the *PATRIOT Act*). On May 17, 2012, one of the MPPs who had raised questions in the Legislative Assembly (the complainant) filed a privacy complaint with my office on this matter, and the issues raised therein form the basis of this report.

Each year, the Ministry sells an average of two million hunting and fishing licences. The licensing system in Ontario requires most individuals to first apply for an Outdoors Card before applying for a hunting and fishing licence. Prior to September 2011, the application process was primarily paper based and there were a number of options available to individuals wanting to apply for a licence. An individual who wanted to apply for an Outdoors Card and a hunting and fishing licence in Ontario could apply by mail, or in person at ServiceOntario, as well as private issuer locations. In some very limited circumstances, a renewal of an Outdoors Card and a hunting and fishing licence could be processed online through the Ministry's website and via an automated telephone system.

If applicants attended at a ServiceOntario location to apply for a licence, a paper application form was completed. ServiceOntario staff (who were granted access to the Ministry's licensing database, referred to as the Outdoors Card Information System (OCIS)), would then manually enter the personal information of applicants into the OCIS database. If applicants attended at a private issuer location, staff at the private issuer would provide the individual with the application form and could assist the applicant in completing this form. The applicant would then mail the application form to the Ministry of Finance, whose staff would input the information into the OCIS database on behalf of the Ministry.

In 2001, through its Recreational Fishing and Hunting Licence Improvement Project, the Ministry retained KPMG Consulting Group (KPMG) to conduct an analysis of the hunting and fishing licensing system. KPMG reviewed the application process and identified opportunities to reduce costs and improve the quality of service being provided to applicants. KPMG made a number of recommendations, the principle one being that the Ministry move to a fully automated licensing process.

In September 2006, the Ministry undertook its own review of the licensing program in light of the KPMG recommendations and made the decision to move to a fully automated system for the sale of hunting and fishing licences. The Ministry completed a conceptual Privacy Impact Assessment (PIA) on this project in July 2007 and received Management Board and Cabinet approval to proceed with the procurement process to select a vendor to operate and manage the automated licensing system on behalf of the Ministry.

In June 2009, the Ministry issued a Request for Proposal to select a vendor for the automated licensing system and in November 2009, it received Management Board and Cabinet approval to award the contract to the successful bidder, Active Outdoors.

Active Outdoors, a publicly traded company, was founded in 1999 and is based in the U.S. Active Outdoors is in the business of providing centralized campground reservations, hunting and fishing licensing, permit sales, point-of-sale and call centre solutions and services for campgrounds, marinas, lodging, and conservation and park agencies.

After the contract with Active Outdoors was signed, and in cooperation with the Office of the Chief Privacy Officer and Archivist of Ontario, the Ministry completed another PIA (October 2010 PIA) on the LAS database in October 2010. The pilot project for the LAS went live in September 2011 and was fully implemented in the spring of 2012.

With the LAS database now in place, the licensing system in Ontario still requires most individuals to first apply for an Outdoors Card before applying for a hunting and fishing licence. Outdoors Cards are issued online, and through 69 ServiceOntario and 850 private issuer locations. Individuals are then able to apply for hunting and fishing licences in three ways: online; by phone through an automated telephone system; or in person at ServiceOntario or private issuer locations. For the purposes of this report, reference to the process of applying for hunting and fishing licences will include Outdoors Cards as well.

Regardless of the method chosen by the applicant, all personal information is entered and stored in the LAS database. The need for paper applications and the subsequent manual entering of personal information has been eliminated.

## The Complaint

The May 17, 2012 letter of complaint raised the following questions about the privacy and security of the personal information stored in the LAS:

- How can the Ministry guarantee the privacy and security of the personal information of applicants when the LAS database is located in a different jurisdiction?
- What other governments or third parties will have access to the data or might be able to gain access?
- What guarantees are there that this private for-profit corporation will not sell or otherwise leverage the information for material gains?
- If the Ministry chooses to terminate its contract with Active Outdoors, who "owns" the data and what guarantees are there that the data would be destroyed?
- Could the information lead to travel problems for hunters and anglers at the U.S. border?

During the course of this investigation, when my office invited the parties to submit additional comments on the issues raised, the complainant raised one additional question:

- What safety mechanisms do the machines operated at Ontario outlets have in protecting personal information from being hacked?

### The Investigative Process

Upon receiving the privacy complaint from the complainant, my office launched an investigation to determine whether the personal information of hunting and fishing licence applicants stored in the LAS database is being collected, used or disclosed in compliance with the *Freedom of Information and Protection of Privacy Act* (the *Act*).

My office initially requested background information on the LAS from the Ministry, which was immediately provided to us. On June 1, 2012, members of my executive team and I held a teleconference with the Deputy Minister and senior officials from the Ministry, at which time further information was provided and additional documentation from the Ministry was requested.

As part of my office's review of this complaint, we received and reviewed relevant documents, including the contract between the Ministry and Active Outdoors for the LAS. We also thoroughly reviewed the Ministry's October 2010 PIA.

During the course of our investigation, the complainant and the Ministry were invited to submit additional comments on any relevant privacy concerns. Throughout this entire investigation, my office received the full and complete cooperation from both the Ministry and the complainant. I would like to commend both parties for providing this office with timely and thorough responses.

## Issues Arising from the Investigation

The issues raised by this complaint are:

1. Is the information at issue "personal information" as defined in section 2(1) of the *Act*?
2. Has the Ministry put in place reasonable measures with respect to the privacy and security of the personal information of applicants for hunting and fishing licences, in accordance with the requirements of the *Act* and its regulations?
3. Is the Ministry's collection of "personal information" in accordance with section 38(2) of the *Act*?
4. Does the Ministry's notice of collection comply with the requirements of section 39(2) of the *Act*?
5. Is the Ministry's use of the "personal information" in accordance with section 41(1) of the *Act*?

For the purposes of the analysis that follows, I find that Active Outdoors, ServiceOntario and the private issuers are agents of the Ministry given that these organizations act on its behalf, in processing hunting and fishing licences. As the complainant has not objected to the involvement of ServiceOntario or the private issuers, I will only comment on the implications of the Ministry's relationship with Active Outdoors (the Agent).

# Discussion

## Issue 1: Is the information in question "personal information" as defined in section 2(1) of the *Act*?

Section 2(1) of the *Act* states, in part, that "personal information" means recorded information about an identifiable individual including:

> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> …
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> …
>
> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

As noted above, the information collected by the Agent and stored in the LAS on behalf of the Ministry includes an applicant's name, date of birth, address and, where applicable, the Outdoors Card number and any information relating to previous suspended hunting and fishing licences. In addition, the Agent collects information that describes the physical characteristics of an applicant, including the applicant's eye colour, height and gender.

There is no dispute that the information in question satisfies the requirements of the definition of "personal information" contained in one or more of paragraphs (a), (c), (d) or (h) of section 2(1) of the *Act*. Having reviewed the program and the application process, I find that the information collected and stored in the LAS qualifies as "personal information."

## Issue 2: Has the Ministry put in place reasonable measures with respect to the privacy and security of the personal information of applicants for hunting and fishing licences, in accordance with the requirements of the *Act* and its regulations?

In determining whether reasonable measures are in place to ensure the privacy and security of the personal information of licence applicants, two issues are significant. First, given that the personal information will be stored in the U.S., what is the impact of the American *PATRIOT Act*? Second, is the contract entered into by the Ministry and its Agent sufficiently robust to provide adequate safeguards for the personal information involved?

### The *PATRIOT Act*

The complainant has expressed concerns that the personal information of Ontarians will be subject to and accessible under American laws, including the *PATRIOT Act*. It is important to remember that, in Ontario, there is no legislative prohibition against the storing of personal information outside of the province or Canada. In other words, Ontario law, including the *Act*, does not speak to this issue. However, the *Act* and its regulations do require provincial institutions to ensure that reasonable measures are in place to protect the privacy and security of their records containing personal information. This applies regardless of where the records are located. Further, Ontario provincial institutions remain accountable for the actions of their agents or service providers, whether located in Ontario or in other jurisdictions.

I understand the complainant's concern that the *PATRIOT Act* may be used by U.S. law enforcement agencies to access Ontarians' personal information. However, the risk that law enforcement agencies may access personal information is not restricted to information held in the U.S. In fact, Canadian law enforcement agencies have similarly robust legal powers to obtain personal information held in Canada, and similar powers exist throughout most countries in the world. Further, law enforcement agencies in Canada, the U.S. and other countries have the ability to reach across borders to access personal information under various laws and agreements.

In this regard, the federal Privacy Commissioner of Canada has found that the privacy risks posed by the *PATRIOT Act* are similar to those found in Canada and, therefore, the privacy protection afforded by a U.S. service provider is comparable to that of a Canadian-based provider.[1] In particular, the federal Privacy Commissioner has stated:

> The risk of personal information being disclosed to government authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, Canadian organizations are subject to similar types of orders to disclose personal information held in Canada to Canadian authorities.[2]

1 *PIPEDA* Case Summary #2005-313. "Bank's notification to customers triggers *PATRIOT Act* concerns." Issued October 19, 2005.
2 *Ibid.*

The federal Privacy Commissioner has also found that prior to the passing of the *PATRIOT Act*, U.S. authorities were able to access records held by U.S.-based firms relating to foreign intelligence gathering in a number of ways, including through formal bilateral agreements.[3]

Canadian legal scholars and practitioners have also carefully examined and commented on the privacy implications of the *PATRIOT Act*. Professor Michael Geist, Canada Research Chair in Internet and E-commerce Law, has written:

> Claims that the enactment of the *USA Patriot Act* has dramatically altered the legal landscape are simply false. The U.S. law enforcement toolkit, which allows for the compelled, secret disclosure of personal information, pre-dates the *USA Patriot Act* by decades. Suggestions that the problem can be solved by keeping personal information from flowing outside the country are not realistic from a real-world, commercial perspective, where data is transferred and stored instantly on computer servers in other jurisdictions without regard for location.[4]

David T.S. Fraser, a prominent Canadian privacy lawyer, has also been very clear in writing:

> Most people are surprised to learn that some of the most "problematic" provisions of the USA *Patriot Act* are replicated in Canadian law in the *Anti-Terrorism Act*. We just don't hear about it as much. People are also surprised to learn of huge amount of information sharing that takes place between agencies in Canada and their counterparts in the US.[5]

The *Act* does not prohibit provincial institutions from outsourcing services on the basis that foreign law, including the *PATRIOT Act*, may apply. Similarly, there is no prohibition on the storage of personal information by government institutions outside the province. In fact, as noted by Professor Geist, outsourcing of technology services is a reality, whether by government agencies or private sector companies. Personal information may be subject to disclosure to law enforcement authorities, whether stored in the province or elsewhere. The critical question for institutions which have outsourced their operations across provincial or international borders is whether they have taken reasonable steps to protect the privacy and security of the records in their custody and control. I have always taken the position that you can outsource services, but you cannot outsource accountability. With this in mind, I now turn to consider what measures the Ministry has put into place in the circumstances of this complaint.

3 *PIPEDA* Case Summary #2008-394. "Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers." Issued August 7, 2008.

4 Michael Geist and Milana Homsi, "Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World," (2005), 54. U.N.B.L.J. 272.

5 David T.S. Fraser, "Patriot Act reality check and Canadian authorities' similar powers" *Canadian Privacy Law Blog* (28 April 2010), online: Canadian Privacy Law Blog <http://blog.privacylawyer.ca/2010/04/patriot-act-reality-check-and-canadian.html>. See also: Michael Power, "**Canada & The PATRIOT Act: Get Over It**" *Michael Power* (31 October 2011), online: Michael Power <http://michaelpower.ca/2011/10/canada-the-patriot-act-get-over-it>.

## The Contract

The complainant has expressed concerns regarding the subcontracting of services and the "safety" of personal information "in the hands of a third party collector," *i.e.* the Agent. The complainant appears to be particularly concerned with the potential misuse or sale of personal information by the Agent. Further, the complainant raises questions regarding the impact of the termination of the relationship between the Ministry and the Agent regarding the personal information held in the LAS database.

As noted above, threats to privacy and security can arise at any time, and in any jurisdiction. Organizations must take reasonable steps to reduce the likelihood of a breach, wherever the information may be held. This becomes especially important when government information management functions are outsourced to private sector agents. In these cases, the reasonable measures required under the *Act* and its regulations include appropriate contractual provisions that ensure accountability, privacy and security. Therefore, whether the Ministry has discharged its obligations to ensure that all reasonable steps have been taken to protect the personal information under its control must be assessed in view of its agreement with the Agent.

I have carefully reviewed the Ministry's agreement with the Agent, including the contract and all appendices and schedules. The Ministry's contract includes robust provisions that protect the personal information under its control and restrict the use of that information by the Agent. In this regard, the following provisions of the contract are relevant:

a) *Ownership* – The contract states that the Ministry shall be the owner of all Ministry data. Ministry data is defined in the contract to include: all data created or modified by the LAS as well as the data relating to licence issuers and angler and hunter licence records, including all data created, modified, collected and stored in the LAS database and any legacy data.

b) *Collection, Use and Disclosure* – The contract states that the Agent cannot directly or indirectly use, collect or disclose any personal information for any purposes not authorized by the Ministry. In particular, the Agent has acknowledged in the contract that unless it obtains specific, written pre-authorization from the Ministry, any access to or use of the Ministry's property, technology or information that is not necessary for the performance of its contractual obligations with the Ministry is strictly prohibited. These restrictions would prohibit the Agent's sale of personal information without the Ministry's consent.

c) *Confidential Information* – Confidential information is defined in the contract to include all personal information that the Ministry is obliged, or has the discretion not to disclose under provincial or federal legislation or otherwise at law. The Agent's contractual obligations for this information include:

    i) keeping the information confidential and secure;

    ii) limiting the disclosure of confidential information to only those who have a need to know it for the purpose of the contract and who have been specifically authorized to receive such disclosure; and

iii) not directly or indirectly disclosing, destroying, exploiting or using any confidential information (except for the purpose of the contract, or except if required by order of a court or tribunal), without first obtaining the written consent of the Ministry and in respect of any of the Ministry's confidential information about any third party, the written consent of such third party.

It is important to note that these restrictions would also prohibit the Agent's sale of personal information without the consent of the Ministry and relevant third party.

d) *Notice of Compelled Disclosure* – **If the Agent is legally compelled to disclose any of the Ministry's confidential information, the Agent must provide the Ministry with prompt notice to allow the Ministry to seek a protective order or other appropriate remedy to prevent or limit such disclosure.** Further, the Agent will disclose only that portion of the confidential information which the Agent is legally compelled to disclose.

e) *Subcontracting* – The contract states that the Agent is not permitted to subcontract the whole or any part of the contract without the prior written consent of the Ministry. If the Ministry does consent to the Agent subcontracting certain services, the Ministry may impose the same contractual obligations on the subcontractor that were imposed on the Agent.

f) *Security* – The contract states that the Agent must ensure the security and integrity of all personal information and records in its possession. The Agent must keep the personal information and records in a physically secure and separate location, safe from loss, alteration, destruction or intermingling with other records and databases. Further, it must implement, use and maintain the most appropriate products, tools, measures and procedures to do so. The Agent has also provided the Ministry with point-of-sale devices that incorporate reliable security, including secure operating and control systems that prohibit any incoming connection to the devices.

g) *Retention and Destruction* – The contract states that the Agent must return all of the Ministry's confidential information to the Ministry before the end of the term of the contract, with no copy or portion kept by the Agent. The Ministry has also stated that it has initiated the development of a retention and destruction schedule with the Agent. The Ministry expects the retention and destruction schedule to be completed by the spring of 2013.

h) *Audits* – The contract states that the Agent will comply with annual audits for privacy and security compliance, for the duration of the contract. These audits may include reviews of threat risk assessments, Privacy Impact Assessments (PIAs) and vulnerability assessments.

i) *Governing law* – The contract clearly states that the governing law of the contract is Ontario and the federal laws of Canada.

With the exception of retention and destruction of the Ministry's data, the Ministry's contract with the Agent demonstrates that the necessary provisions are in place to strongly safeguard the privacy and security of personal information collected under the hunting and fishing licensing

program. The contract includes provisions that address the collection, use and disclosure of personal information, auditing, subcontracting of services, ownership and security of the data. Specifically, in terms of the questions raised by the complainant, the contract clearly states that the personal information is owned by the Ministry and that access to the data is strictly circumscribed. The Agent is not allowed to use the data for its own purposes, for example, by selling the data to third parties. Further, clear rules are in place should the contract be terminated. In addition, the security of point-of-sale devices has also been addressed.

I have recommended that the Ministry finalize its retention and destruction schedule with the Agent as soon as possible and no later than December 31, 2012. The Ministry has agreed to implement this recommendation. Subject to this recommendation, I am satisfied that the Ministry has put in place reasonable measures to protect the personal information provided to the Agent, in accordance with the *Act* and its regulations.

## Issue 3: Is the Ministry's collection of "personal information" in accordance with section 38(2) of the *Act*?

The Ministry agrees that the current licensing application process for hunting and fishing licences involves the collection of personal information by the Ministry. This collection takes place when an individual makes an application for a licence. Although the authority for the collection of personal information has not been questioned by the parties, for the sake of completeness, I will address that issue in the discussion that follows.

Section 38(2) of the *Act* sets limits on the circumstances in which personal information may be collected on behalf of an institution, whether directly or indirectly. In order for a collection to be permissible under section 38(2) of the *Act*, the institution must demonstrate that it meets at least one of the three conditions listed in that section which states:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

The Ministry's October 2010 PIA states that the personal information at issue is collected under the express statutory authority of the *Fish and Wildlife Conservation Act, 1997* (*FWCA*), and is necessary to the proper administration of a lawfully authorized activity.

Sections 60 and 61(1) of the *FWCA* give the Minister of Natural Resources the authority to issue licences for the purposes of the *FWCA* and the authority to authorize others to issue the licences on its behalf. Those sections state:

60. The Minister may issue licences for the purposes of,

(a) this *Act*; and

(b) the Ontario Fishery Regulations.

61. (1) The Minister may authorize a person to issue licences on the Minister's behalf.

Section 69 of the *FWCA* states that no person shall possess a licence that does not identify the holder of the licence, and section 82(1) states that the minister may establish the form or format of any licence issued under the *FWCA*.

Reading these sections of the *FWCA* together, I am satisfied that the Ministry has the express statutory authority to collect personal information for the purposes of its licensing program. I also find that the collection of each item or class of personal information at issue, including the applicant's name, contact details and physical description, is necessary to properly administer this lawfully authorized activity.

For these reasons, I find that the Ministry is collecting personal information in compliance with section 38(2) of the *Act*.

## Issue 4: Does the Ministry's notice of collection comply with the requirements of section 39(2) of the *Act*?

Under the *Act*, an institution is required to provide individuals with formal notice of the collection of their personal information. The purposes of the notice are to ensure that an institution's practices with respect to personal information are transparent and that an institution is accountable to the individual. In addition, the notice of collection may serve to reduce any concerns regarding the collection and use of personal information.

This notice requirement and the necessary elements of the notice are set out in section 39(2) which states:

> Where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of,
>
> (a) the legal authority for the collection;
>
> (b) the principal purpose or purposes for which the personal information is intended to be used; and
>
> (c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

At the time that this complaint was filed, the notice of collection that was in use by the Ministry for online and in-person applicants stated:

> Personal information is collected under the authority of the *Fish and Wildlife Conservation Act, 1997*, SO 1997 and will be used for the purposes of identification, enforcement, research and administration. While personal information may be stored outside Canada and subject to the laws of the jurisdiction where it is

> stored, private companies under contract to provide the licensing services are contractually obligated to comply with Ontario's *Freedom of Information and Protection of Privacy Act* with regard to personal information in their custody. For information about collection practices contact the Outdoors Card Centre Team Lead, Outdoors Card Centre, Fish and Wildlife Services Branch, Ontario Ministry of Natural Resources, 300 Water Street, Peterborough, Ontario, K9J 8M5, 1 (800)-387-7011.

The notice of collection that was used on the automated telephone application process stated:

> Personal information is collected under the authority of the *Fish and Wildlife Conservation Act, 1997,* SO 1997 and will be used for the purposes of identification, enforcement, research, marketing and administration. Personal information may be stored outside of Canada and subject to the laws of the jurisdiction where it is stored. For information about collection practices, contact the Outdoors Card Centre at 1-800-387-7011.

The notice used in the online application appears on the first page of the application form. When applying via the automated telephone system, the notice is read out to the caller. In the event that an individual applies at a ServiceOntario location or at a private issuer location, the notice is provided in poster format.

The Ministry provided my office with a Frequently Asked Questions (FAQ) document that is used by Outdoors Card Centre staff as a tool to assist them in answering questions that they may receive from individuals about the Ministry's collection practices. The FAQ includes information about how the *Act* applies to personal information stored in the U.S., how the Ministry uses the personal information gathered, and the steps that the Ministry has taken to protect the privacy of applicants.

When I was initially contacted about the LAS system, I personally reviewed the notices of collection that were in use online, by phone and in-person, to determine whether they accorded with the requirements in section 39(2). I immediately expressed a number of concerns about the notices of collection at that time and, as a result, changes were made to the notices on an interim basis. Subsequently, in discussions that my staff had with the Ministry, it was acknowledged that the notices of collection required further amendments, and the Ministry agreed to work with my office to amend them.

My initial concerns about the notices were threefold. First, the notices of collection stated that the personal information collected "will be used…for marketing." Given that the Ministry had established an opt-in or consent-based approach to its use of personal information for marketing purposes, it was simply not accurate to state that the personal information "will be" used for marketing. The default condition was that it would be used for marketing unless the individual positively consented and "opted-in." I will discuss the opt-in approach in greater detail below. However, it is sufficient to note here that since the original notice did not accurately reflect the Ministry's practice, I advised the Ministry to completely remove the reference to "marketing" from the notices.

Second, I was also concerned that the notices of collection stated that personal information "may be stored outside of Canada" as it was clear that the Agent **was** storing some of applicants' personal information in the U.S. During this investigation, it was confirmed that applicants' financial information (e.g. credit card number) collected to process the licence transaction would **never be** stored in the U.S. Consequently, I advised the Ministry that the notice of collection should state that "some of the applicants' personal information will be stored outside of Canada." This accurately reflects the fact that some, but not all of the personal information collected as part of the licensing program, will be stored in the U.S.

Third, the notice of collection used in the automated telephone application process did not provide the title and business address of a public official who could answer questions about the collection as required by section 39(2)(c) of the *Act*. Accordingly, I advised the Ministry to add this information to the notice used in this automated system. I note that other changes to this notice were made during this investigation to ensure consistency with the notice that is used in the online and in-person application process.

I also note that, at the time of writing this report, changes to the poster used at private issuers have been implemented but that changes to the poster used at ServiceOntario locations have not been made. However, the Ministry has undertaken to make those changes and reprint these posters at the earliest opportunity. The Ministry aims to have the revised posters on display at ServiceOntario locations by the end of July 2012.

In summary, during the course of my investigation, I made recommendations for changes to the notices of collection which the Ministry has either implemented or has committed to implementing. In these circumstances, and subject to the implementation of new posters for use in ServiceOntario locations, I am satisfied that the revised notices of collection comply with the requirements of section 39(2) of the *Act*.

## Issue 5: Is the Ministry's use of the "personal information" in accordance with section 41(1) of the *Act*?

Section 41(1) of the *Act* imposes a general prohibition on the use of personal information, but states that personal information may be used in a number of enumerated exceptional circumstances. That section states, in part:

> An institution shall not use personal information in its custody or under its control except,
>
> (a) where the person to whom the information relates has identified that information in particular and consented to its use;
>
> (b) or the purpose for which it was obtained or compiled or for a consistent purpose;

With respect to the term "consistent purpose" found in section 41(1)(b), section 43 states:

> Where personal information has been collected directly from the individual to whom the information relates, the purpose of a use or disclosure of that

> information is a consistent purpose under clauses 41(1)(b) and 42(1)(c) only if the individual might reasonably have expected such a use or disclosure.

In order for a given use of personal information to be permissible under the *Act*, the institution in question must demonstrate that the use was in accordance with at least **one** of the section 41(1) exceptions.

## Section 41(1)(a)

As the limitations on the Agent's use of the personal information are governed by the contract and are set out above, I will only address here the issues arising out of the Ministry's use of the information. Among other things, as indicated, the Ministry is proposing to use the personal information collected through its Agent for the purposes of "marketing." It provided the following information regarding this use:

> Important to note, the MNR does NOT directly provide client information to any third parties for marketing purposes. In full disclosure, as part of a revenue generating initiative, the MNR conducts an internal direct mailing 2-3 times a year in which the Fish and Wildlife Services Branch sells available space in their client mailings to interested third parties. This space usually consists of a commercial insert that is made to accompany MNR communications material. Currently, the MNR has entered reciprocal agreements with two publications in Ontario. In exchange for ad space in their publications, the MNR authorizes them to participate in approved direct mailing campaigns and only target those clients who have opted-in to receive commercial mailings. As stated above, in this case, there is NO disclosure of personal information and the MNR only targets those clients who have opted for commercial mailings.

When individuals make an application for a licence, they are asked to consent to their personal information being shared by the Ministry with commercial businesses for solicitation by mail or email. For those applying in person or online, the opt-in portion of the application is set out in two parts:

> By checking this box the customer authorizes MNR to share my information with Commercial Businesses for possible mailings solicitation. ☐
>
> By checking this box the customer authorizes MNR to share my information with Commercial Businesses for possible e-mail solicitation. ☐

Individuals renewing their licence using the automated telephone system are asked if they consent to their personal information being used by the Ministry for commercial mailings. At the end of the automated telephone process, applicants are asked to "press 0" if the Ministry may, "use (their) name and address for commercial mailings relating to hunting and fishing" or to "press 1" if they do not wish the Ministry to use their personal information for such mailings. Therefore, the opportunity to provide opt-in consent exists regardless of which method individuals choose.

The Ministry has confirmed with my office that applicants' personal information is only used for solicitation purposes by commercial businesses if applicants explicitly opt-in or consent to their information being used for this purpose. Importantly, this means that the default privacy setting used by the Ministry is that personal information is not shared with third parties.

In these circumstances, I am satisfied that the use of personal information at issue for solicitation by commercial businesses or marketing is consistent with section 41(1)(a) of the *Act* since the person to whom the information relates has consented to this use.

## Section 41(1)(b)

In addition to potentially using personal information for marketing, the Ministry is also using the information for the purposes of identification, enforcement, research and administration. Section 41(1)(b) of the *Act* is raised as the authority for this use on the basis that these are the same purposes for which the personal information is obtained and compiled or are consistent purposes.

In determining whether a given use of personal information is in accordance with section 41(1)(b), it is first necessary to determine the original purpose of the collection. It is then necessary to assess whether the use of this information can be properly characterized as being either for the original purpose of the collection, or for a purpose that is consistent with that original purpose.

The final step in the section 41(1)(b) analysis is to look to section 43 of the *Act*, which provides clarification on whether a given use of personal information constitutes a "consistent purpose" by imposing a "reasonable person" test. Therefore, the question that must be asked is whether an individual in the position of applying for a licence would have reasonably expected the use of their personal information for the identified purposes. Previous complaint reports issued by my office have found that there must be a rational connection between the purpose of the collection and the purpose of the use in order to meet the "reasonable person" test [Report MC07-64].

In this case, I note that the personal information collected on the licence application is collected for the purpose of administering the application process and, more particularly, for the purpose of including identifying information on the licence as required by section 69 of the *FWCA*. Other personal information is collected for the purpose of enforcement and communications with the applicants regarding the licensing program.

I am satisfied that the use of personal information for identification, enforcement, and administration are integral parts of the administration of the licensing program and, therefore, the same purposes for which the personal information is obtained or compiled.

With respect to the Ministry's use of personal information for research purposes, the Ministry states:

> Collection and analysis of demographical data will allow the MNR to achieve a better understanding of their client base, improve efficiency in service delivery, and overall, improve client satisfaction by building targeted communications based on their clients' needs.

In my view, applicants for hunting and fishing licences could reasonably expect the use of their personal information for the purpose of Ministry research conducted to "improve efficiency in service delivery" and "client satisfaction." The fact that an organization may use the personal information it collects for this type of research is not surprising and, in my view, there exists a rational connection between this use and the original purpose for which the information was collected. Accordingly, I am satisfied that the use for research is a "consistent purpose."

For the reasons set out above, I find that the Ministry's use of personal information for the purposes of identification, enforcement, research and administration is in compliance with section 41(1)(b) of the *Act*.

## Conclusion

In summary, I conclude that:

1. The information in question is personal information as defined in section 2(1) of the *Act*.
2. The Ministry has agreed to finalize its retention and destruction schedule as soon as possible but no later than December 31, 2012 in accordance with my recommendation. Subject to this, the Ministry's contract with its Agent demonstrates that the necessary provisions are in place to safeguard the privacy and security of the personal information in the LAS as required under the *Act* and its regulations.
3. The Ministry's collection of the "personal information" is in accordance with section 38(2) of the *Act*.
4. The Ministry has agreed to implement my recommendations for changes to the notices of collection to ensure compliance with section 39(2) of the *Act*.
5. The Ministry's use of the "personal information" is in accordance with section 41(1) of the *Act*.

## Summary

I have found that the Ministry's collection, use and disclosure of personal information for the purpose of administering the Ministry's hunting and fishing licensing program is in compliance with the *Freedom of Information and Protection of Privacy Act*. In addition, I have found that the Ministry's contract with Active Outdoors is comprehensive, and includes sufficient provisions to safeguard the privacy and security of personal information, and to restrict the use of this personal information by the Agent, in accordance with the *Act*.

During this investigation, I made several recommendations for changes to the notices of collection that were previously in use by the Ministry. The Ministry has agreed to follow all of these recommendations. Once fully implemented, the notices of collection will be in compliance

with the requirements of the *Act*. I have also recommended that the Ministry expedite its plan to develop retention and destruction schedules, and it has agreed to do so.

In arriving at my findings regarding the privacy and security of the personal information that is stored in the LAS database, I have considered the complainant's concerns regarding the outsourcing of the licensing application process and the implications of the *PATRIOT Act*. I have found that there is no provision in the *Act* which precludes an institution from outsourcing services; the passage of the U.S. *PATRIOT Act* does not alter that view. Regardless of whether or not an Ontario government institution decides to outsource an activity that involves the collection, use and disclosure of the personal information of Ontarians, full accountability for privacy and security of the information remains with the government institution.

Importantly, many of the privacy risks posed by the *PATRIOT Act* existed prior to the enactment of that legislation. I agree with the comments of Professor Geist, quoted above, that the *PATRIOT Act* has not "dramatically altered the legal landscape." Institutions are permitted to outsource their operations across provincial and international borders, provided that reasonable safeguards are implemented to protect the privacy and security of the information at issue. Crucial to these safeguards is the implementation of strong contractual provisions that help to ensure compliance with the *Act* – strong safeguards, which are clearly present in the circumstances of this complaint.

## Commissioner's Message

There may be no greater area of confusion and misunderstanding than fear of the *PATRIOT Act*. The *PATRIOT Act* has invoked unprecedented levels of apprehension and consternation – far more than I believe is warranted. For the reasons outlined on pages 5 and 6, the feared powers were available to law enforcement long before the passage of the *PATRIOT Act*, through a variety of other legal instruments. In my view, these fears are largely overblown, and focusing on them unduly constitutes a pointless exercise. I believe it is far more productive to compel organizations to be fully responsible and accountable for the services they provide or outsource. As noted earlier, my position on this remains that you can outsource services, but you cannot outsource accountability. Flowing from that, one critical question prevails: Have reasonable steps been taken to ensure privacy and security, regardless of where the data resides? The measures taken by MNR, as described in this report, represent a good example of such accountability.

June 27, 2012

Ann Cavoukian, Ph.D.
Commissioner

Date

**Information & Privacy Commissioner of Ontario**
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada
416-326-3333 1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca
Email: info@ipc.on.ca