IPC
PERSPECTIVES
INFORMATION AND PRIVACY COMMISSIONER / ONTARIO

VOLUME 17
ISSUE 1
2007

ANN CAVOUKIAN, Ph.D., COMMISSIONER

Commissioner Ann Cavoukian makes a point at the news conference the IPC held in October to unveil the **Privacy-Embedded 7 Laws of Identity.** She is flanked by Peter Cullen, Microsoft's chief privacy strategist (left) and Kim Cameron, chief identity architect for Microsoft.

Commissioner Cavoukian unveils blueprint for privacy-embedded Internet identity

By Ann Cavoukian, Ph.D
Information and Privacy Commissioner/ Ontario

There is a growing disjunct between the real and online worlds. In the bricks-and-mortar world we live in, we identify ourselves to others according to context and preferences: presenting cash or a coffee card for our coffee; a membership card gains access the gym facilities; a passport allows us to cross the border. Different ID cards are in our wallets, and we are in control of the personal information we disclose to others. In the real world, we can also verify who the other party is before revealing our own identity.

In the digital realm, we have far less control. Online tracking and surveillance, excessive collection of personal information, and online fraud are becoming much more the norm. Consumers are beginning to lose confidence and trust in the online medium, and are starting to drop out. Part of this problem is that there is no convenient way for people to manage their various identities and their privacy online as effectively as they do offline.

On October 18, I announced my support for a global online identity system framework by unveiling far-reaching "privacy-embedded" laws, which would help consumers verify the identity of legitimate organizations before making online transactions.

These laws were inspired by, and map to, the *7 Laws of Identity*, formulated through a global dialogue among security

CONTINUED ON PAGE 4

In this issue:

Recent IPC Publications

The IPC has issued (in order of publication) the following publications since the last edition of *IPC Perspectives:*

Get together, win together: Mediation at the IPC (video). May 2006.

Privacy Guidelines for RFID Information Systems. June 2006.

Practical Tips for Implementing RFID Privacy Guidelines. June 2006.

Commissioner Ann Cavoukian's 2005 Annual Report. June 2006.

What to do When Faced With a Privacy Breach: Guidelines for the Health Sector. July 2006.

If you wanted to know…How to access your personal information held by a municipal organization. September 2006.

Reduce Your Roaming Risks: A Portable Privacy Primer. September 2006.

When Online Gets Out of Line: Privacy – Make an Informed Online Choice. October 2006.

7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age (paper and brochure). October 2006.

Breach Notification Assessment Tool. December 2006.

All of these publications and more are available on the IPC's website at **www.ipc.on.ca.**

Upcoming Presentations

February 9, 2007.

Commissioner Ann Cavoukian is meeting with the CBC editorial board to discuss ongoing and evolving privacy and access issues.

February 13, 2007.

Commissioner Cavoukian is addressing the Arizona Association of Certified Fraud Examiners. Her topic: *Privacy and Security: Bringing Both into Alignment.*

February 16, 2007.

Commissioner Cavoukian is the keynote speaker at the *B.C. Privacy and Security Conference* at the Victoria Conference Centre.

February 27, 2007.

Commissioner Cavoukian is a special guest speaker at the University of Waterloo. The focal point of her address is privacy issues related to identity.

March 7, 2007.

Commissioner Cavoukian is making a special presentation on access and privacy to the Canadian Armenian Business Council.

May 15, 2007.

Commissioner Cavoukian is a keynote speaker at the Canadian Marketing Association's national conference. Her topic: *Make Privacy Work for You: Gain a Competitive Advantage.*

Canada's first *Right to Know Week* marked

Ontario Information and Privacy Commissioner Ann Cavoukian worked with her counterparts across Canada, and the federal Information Commissioner, to jointly create – and mark – Canada's first *Right to Know Week* in late September, to help build public awareness of citizens' rights to public information.

The timing was based on the international Right to Know Day, September 28. As the Commissioner told a sold-out *Right to Know Week* luncheon at the Ontario Club, it was on Sept. 28, 2002, that Freedom of Information organizations from various countries around the globe met in Sofia, Bulgaria, created a network of Freedom of Information Advocates and agreed to collaborate in the promotion of individuals' right of access to information and open, transparent government.

"The right of citizens to access government-held information is absolutely essential," said Commissioner Cavoukian. "Otherwise, citizens cannot hold elected and appointed officials accountable to the people they serve. Without openness and accountability, you cannot have a strong democratic society."

The Commissioner served as the moderator for a special panel at the *Right to Know Week* luncheon, which was organized by the IPC and co-sponsored by the Canadian Newspaper Association and the Toronto Region branch of the Institute of Public Administration of Canada.

Commissioner Cavoukian stressed that her foundation message to Ontario's provincial and municipal government institutions is that "exemptions to the release of information should not be claimed routinely just because they are technically available. They should only be claimed if they genuinely apply. The default position should always be disclosure."

The three panellists included Brian Beamish, IPC Assistant Commissioner (Access), Anne Kothawala, president and CEO of the Canadian Newspaper Association (CNA), and Robert Cribb, an award-winning *Toronto Star* reporter and past-president of the Canadian Association of Journalists.

Beamish, who outlined the role of the IPC as the appeal level in the freedom of information process, stressed the importance of government transparency.

Kothawala told the predominantly civil servant audience some of the problems that a recent FOI audit sponsored by the CNA had uncovered. Reporters from 40 newspapers or news agencies across Canada had gone to municipal and federal offices seeking specific types of information – first through over-the-counter requests, then through formal FOI requests if the informal approach was rejected. While the information sought was released in some cases – release of the same type of information was denied in others. (For more information: **http://www.cna-acj.ca/Client/CNA/cna.nsf/web/CNA+releases+2006+FOI+Audit?OpenDocument.**)

Cribb, who was directly involved in helping to plan for and then review the results of the audit, said some government officials simply did not understand that Canadians have a right of access to the information held by governments.

IPC Adjudicator Steve Faughnan was presented with a recognition award by the Society of Ontario Adjudicators and Regulators (SOAR) at its recent annual Conference of Boards and Agencies, which is attended by chairs, vice-chairs and members of Ontario's adjudicative and agency community. One of four recipients of the award, it was given to Faughnan in recognition of his past work as a member of SOAR's education committee and as inaugural chair of the adjudicator training course revamp sub-committee.

Commissioner unveils blueprint for privacy-embedded Internet identity

CONTINUED FROM PAGE 1

and privacy experts, headed by Kim Cameron, Chief Identity Architect at Microsoft. The *7 Laws of Identity* proposed the creation of a revolutionary "identity layer" for the Internet, providing a broad conceptual framework for a universal, interoperable identity system.

The *Privacy-Embedded 7 Laws of Identity* that I unveiled in October incorporate additional key insights from the privacy arena. An extension of the original *7 Laws*, they encourage privacy-enhanced features to be embedded into the design of IT architecture and be made available early in the emerging universal identity system.

The Internet was built without a way to know who and what individuals are connecting to. This limits what people can do and exposes computer users to potential fraud. If the IT industry and government do nothing, the result will be rapidly proliferating episodes of theft and deception that will cumulatively erode public trust. That confidence is already eroding as a result of spam, phishing and identity theft. The *Privacy-Embedded 7 Laws of Identity* supports the global initiative to empower consumers to manage their own digital identities and personal information in a much more secure, verifiable and private manner.

Just as the Internet saw explosive growth as it sprang from the connection of different proprietary networks, an "Identity Big Bang" is expected to happen once an open, non-proprietary and universal method to connect identity systems **and** ensure user privacy is developed in accordance with privacy principles. Microsoft started a global privacy momentum. Already, there is a long and growing list of companies and individuals that now endorse the *7 Laws of Identity* and are working towards developing identity systems that conform to them.

The privacy-enhanced laws will help to minimize the risk that one's online identities and activities will be linked together.

Just as important, identity systems that are consistent with the *Privacy-Embedded 7 Laws of Identity* will help consumers verify the identity of legitimate organizations before they decide to continue with an online transaction.

The next generation of intelligent and interactive web services ("Web 2.0") will require more, not fewer, verifiable identity credentials, and much greater mutual trust to succeed.

In brief, the *Privacy-Embedded 7 Laws of Identity* offers individuals:

- easier and more direct user control over their personal information when online;
- enhanced user ability to minimize the amount of identifying data revealed online;
- enhanced user ability to minimize the linkage between different identities and actions;
- enhanced user ability to detect fraudulent messages and websites, thereby minimizing the incidence of phishing and pharming.

We have called upon software developers, the privacy community and public policy-makers to consider the *Privacy-Embedded 7 Laws of Identity* closely, to discuss them publicly, and to take them to heart.

Many have already taken us up on our call, stepping forward to present their own identity management projects and to explain how their solutions are user-centric, privacy-respecting and privacy-enhancing. The IPC is currently in talks with several collaborative, open-source identity management initiatives, such as members of Liberty Alliance (which includes such companies as Sun and Oracle) and members of Project Higgins (which includes IBM and many others), to further advance individual privacy in the identity age.

More information about the *Privacy-Enhancing 7 Laws of Identity* is available at: www.ipc.on.ca/index.asp?navid=67&fid1=15.

Commissioner Ann Cavoukian addresses Powerpoint Group's **Women of Influence** September luncheon at the Fairmount Royal York Hotel. Her talk, **Defy the Odds**, about the challenges she personally has had to overcome, attracted a sold-out audience.

IPC relaunches its quickly growing website

The IPC relaunched its website in October, after an extensive makeover, to help make it easier for visitors to find specific types of information on the quickly growing site.

For example, since the IPC has more than 5,000 orders and investigation results posted, the new website offers various ways to refine a search using various indices.

To find the **Subject Index** (orders or investigations related to a particular topic) or **Section Indices** (orders or investigations related to a specific section of one of the *Acts)*, click on **Decisions & Resolutions.**

On the left side of the new page, you will see two tabs: **Browse by Legislation** and **Browse by Subject.**

If you want a **Section** Index, click on **Browse by Legislation,** then on:

- whichever one of the three *Acts* (*Freedom of Information and Protection of Privacy Act,* the *Municipal Freedom of Information and Protection of Privacy Act* or the *Personal Health Information Protection Act*) applies,
- then click on the plus sign, which will bring up the Section Index for that *Act*. As a bonus, the right-hand column cross-references the results with the Subject Index.

For example, if you select the provincial *Act* (*FIPPA*) and then click the **plus (+) sign** to bring up the Section Index for that *Act*, you can then click on the section or subsection you are interested in – say, section 15. You will see there are seven orders related to this section. (These orders relate to section 15 specifically and do not include orders relating to its subsections.)

The right-hand column contains a list of the subjects that the seven orders cover. One subject is cabinet records (two orders). If someone was looking for orders related to section 15 **and**

Continued on Page 9

Protect the information you take out of the office

Minimize and secure the data before leaving the office.

But if you do lose – or have the personal information of clients or staff stolen – act immediately.

These are two of the key messages in *Reduce Your Roaming Risks: A Portable Privacy Primer*, produced jointly by the IPC and BMO Financial Group and released in September.

There have been a number of news reports over the past couple of years of large privacy breaches, when portable computers or other devices holding the personal information of thousands are either lost or stolen.

This brochure provides a series of checklists and steps to take to reduce the chances of a privacy breach occurring when people are working with personal information away from the traditional office setting.

"Our consistent message has been that organizations must step up and take action to help prevent breaches of information which can lead to identity theft," said Information and Privacy Commissioner Ann Cavoukian. "This very practical, hands-on brochure can be a key tool; it helps to create what we call a culture of privacy. I applaud BMO for embracing this approach."

Among the recommendations that the Commissioner and BMO make in the brochure:

- Always use strong password protection, preferably in conjunction with data encryption;
- Do not remove any client information from your organization's network or premises without proper authorization from your supervisor;
- Remove all confidential information, or any devices containing confidential information, from plain sight in your vehicle. Lock your valuables in the trunk **before** you start the trip, not in the parking lot of your destination;
- In public places, do not discuss any confidential information on your cell phone; and
- Only conduct confidential business on business or personal computers. Do not use public computers or networks, or conduct business in public places.

Laptops, PDAs and, more recently, cell phones, are considered to be the "golden eggs" by identity thieves.

Here are some of the precautions the brochure recommends be taken to minimize the risks:

- Ensure that all of your devices require passwords for access: power-on passwords, screensaver passwords, account passwords. Strong passwords consist of at least eight characters, upper and lower case, numerals and special characters. The password should not be a word that can be found in any dictionary;
- Enable the automatic lock feature of your device after five minutes of idle time;
- Encrypt your data according to your company's policies. This is essential if you transport personal and/or confidential customer data – it should never be left in "plain view;"
- When no longer needed, remove all confidential data from your devices using a strong "digital wipe" utility program. Do not simply rely on the "delete" function;
- If you handle confidential information online or perform financial transactions, then your laptop (and sometimes your PDA) should, at a minimum, have a personal firewall, anti-virus and anti-spyware protection. In addition, install the latest updates and security patches for your mobile devices, including your cell phone;
- When connecting to public wireless networks or HotSpots in airports, hotels, coffee shops, etc., bear in mind that these networks are inherently unsafe. Remember the following:
    - Watch out for shoulder surfing – someone "casually" observing the work on your laptop;
    - Never connect to two separate networks simultaneously (such as Wi-Fi and Bluetooth);
    - Do not conduct confidential business unless you use an encrypted link to the host network (such as a Virtual Private Network – VPN).

The brochure also contains advice on what to do if you lose confidential data – your own and/or that of clients (take immediate action!) – as well as providing a quick reference checklist.

Reduce Your Roaming Risks is available on the IPC's website at **www.ipc.on.ca**.

Students urged to think about privacy when selecting a social networking site

Commissioner Ann Cavoukian spoke about privacy and social networks to open the **Ethics at Ryerson Speaker Series** at Toronto's Arts and Letters Club in October. With her, just prior to her presentation, are (from left), Assistant Privacy Commissioner Ken Anderson, Chris Kelly of Facebook, privacy consultant and former U.S. Federal Trade Commissioner Mozelle Thompson, and Brian Jensen and Ifoma Smart of Privasoft.

Online social networking sites – where individuals can post all kinds of personal information about themselves and their friends, including pictures – have become a social and technological phenomenon.

After media coverage of problems sparked by some of these public postings, Commissioner Ann Cavoukian became concerned that many of the college and high school students who flocked to some of the more prominent sites were not fully aware of what posting some types of personal information – without considering privacy options – could mean.

There were media reports about incidents of stalking or identity theft. And there were also other issues that were not always immediately apparent. Photographs of students at wild parties, or posing in questionable situations, can result in prospective employers screening out potential employees. (More and more companies are doing web searches on prospective employees, according to several surveys.) And it is not just photos. What seems at the time to be witty social commentary or satirical political comments posted on a person's publicly viewable profile have been used as grounds for termination or denial of employment.

Despite most online social networking websites having privacy policies and optional settings that can limit access to sensitive information, the Commissioner discovered that many students were often not taking the time to investigate the privacy choices they had online.

Commissioner Cavoukian sat down with a small focus group set up by the IPC (students from six Canadian universities) to discuss the students' use of social networking websites, whether any had ever read the privacy options, any concerns they might have for their privacy and other related issues. "This was a great session," said the Commissioner. "They were all so bright, so open to this discussion ... but they were not worried about their privacy and had not taken the time to consider privacy options before starting to post personal information on these websites."

Continued on Page 9

PHIPA order cites a "blatant disregard" for the privacy of a hospital patient

Commissioner Ann Cavoukian issued her second order under Ontario's *Personal Health Information Protection Act* (*PHIPA*) in July, following an investigation into a serious breach of a patient's privacy at the Ottawa Hospital.

A patient had informed the staff that she did not want her estranged husband and his girlfriend, both employees of the hospital, to be made aware of her admittance or to have access to her personal health information.

What occurred was the exact opposite, as the girlfriend of the patient's estranged husband – a nurse who was not involved in the patient's treatment – was able to access the patient's hospital records – both before and after the initial violations were brought to the attention of hospital officials.

Upon receiving the complaint, the hospital took immediate steps to flag the patient's electronic health record (EHR) and an audit confirmed that her estranged husband's girlfriend had inappropriately accessed her EHR. However, the hospital did not take immediate steps to prevent the nurse from gaining further unauthorized access to the patient's health information. The Commissioner's investigation concluded that the nurse inappropriately accessed the patient's EHR on three occasions after the complaint was made.

The Commissioner concluded that the nurse, as an employee of the hospital, "used" the information in contravention of *PHIPA*. The hospital itself violated *PHIPA* by not following internal hospital policies related to the protection of patients' privacy, and failing to take immediate action to prevent any further unauthorized use of the patient's personal health information.

In HO-002, the Commissioner ordered:

- the hospital to review and revise its practices, procedures and protocols relating to patient health information and privacy, and those relating to human resources, to ensure that they comply with the requirements of the *Act* and its regulations, taking into account the concerns expressed in this order about the paramount importance of protecting patients' personal health information;
- that the hospital, as part of the review under order provision, implement a protocol to ensure that reasonable and immediate steps are taken, upon being notified of an actual or potential breach of an individual's privacy, to ensure that no further unauthorized use or disclosure of records of personal health information is permitted;
- following the review, that the hospital ensure that all employees and/or agents of the hospital are appropriately informed of:
  (a) their duties under the *Act* pursuant to section 15(3)(b) of the *Act*;
  (b) their obligations to comply with the revised information practices of the hospital pursuant to section 10(2) of the *Act*.

The Commissioner also urged the hospital to issue a formal apology to the complainant.

As part of a postscript to her order, the Commissioner said:

"…Despite having alerted the hospital to the possibility of harm, the harm nonetheless occurred. While the hospital had policies in place to safeguard health information, they were not followed completely, nor were they sufficient to prevent a breach of this nature from occurring. In addition, the fact that the nurse chose to disregard not only the hospital's policies but her ethical obligations as a registered nurse, and continued to surreptitiously access a patient's electronic health record, disregarding three warnings alerting her to the seriousness of her unauthorized access, is especially troubling. Protections against such blatant disregard for a patient's privacy by an employee of a hospital must be built into the policies and practices of a health institution."

"This speaks broadly to the culture of privacy that must be created in healthcare institutions across the province. Unless policies are interwoven into the fabric of a hospital's day-to-day operations, they will not work. Hospitals must ensure that they not only educate their staff about the *Act* and information policies and practices implemented by the hospital, but must also ensure that privacy becomes embedded into their institutional culture."

Students urged to think about privacy when selecting a social networking site

CONTINUED FROM PAGE 7

In October, the Commissioner and Facebook.com, a large social networking site, launched a joint brochure, *When Online Gets Out of Line: Privacy – Make an Informed Online Choice*. The brochure focuses on informing students about how personal information posted on a social networking website today could result in future consequences – whether it be employment or educational repercussions, reputation damage, or even stalking. The brochure urges all users of online social networking websites to inform themselves about their privacy settings on all websites, to actively use those privacy settings, and to constantly review a website's privacy policy.

The message the Commissioner is conveying through the brochure – and in presentations and interviews – is "control." Only a user can control the privacy settings on a social networking website, only a user can control what information to post or not to post online. Above all, the brochure stresses that the final decision to post personal information online rests with the individual, but each person should make an informed choice before doing so.

The Commissioner launched her online social networking initiative and the brochure at Ryerson University's *Ethics at Ryerson* speaker series Oct. 12, to a group of business professionals, university professors, and university and college students. Thousands of copies of the brochures have been distributed to universities and colleges across Ontario, and other provincial privacy commissioners have also used the IPC brochure in public awareness campaigns relating to online social networking.

Commissioner Cavoukian has also taken this initiative to high school students – making a presentation at Bishop Strachan School in Toronto in early December, where she spoke on the topic of cyber-bullying. The Commissioner outlined the potential impact of online activities, including what the long-term consequences could be. Her key message: "Anything posted online can stay online forever and may be searched by teachers, university administrators, or prospective employers. This information creates an 'online résumé' that you will not be able to control." Before posting anything on the Internet, urged the Commissioner, "Think, before you click."

IPC relaunches its website

CONTINUED FROM PAGE 5

cabinet records, he or she would only need to check the two orders, rather than all seven.

If you want to search using the **Subject Index,** click on **Browse by Subject.**

Select the subject you are interested in (click the plus sign to expand a subject). If you click on Advice or Recommendations, the first 10 of the 105 orders related to this subject will be displayed in the middle of the screen. (You can scroll through all 105, if desired.) In the right-hand column, the orders will be cross-referenced by the Section Indices. If the searcher wants to know how a particular section applies to the subject he or she has selected, he/she can click on the section, which will refine the results (reducing those 105 orders down to the number related to **both** the section and subject).

There is a wide variety of information posted on the website, from IPC publications to submissions to news releases to presentations to "how to" information. If, for example, you want to learn how to file an **appeal** or a **privacy complaint** to the IPC, or how the IPC deals with these, just click on **About Us**, one of the main menu options at the top of the page, then click on **IPC Procedures.**

There is a multi-level search function allowing you to do a quick search of the site using the search box at the top-right corner of the screen, browse publications and orders, or do an Advanced Search. However, if you are unsure exactly what you are looking for, or just browsing, you can go to the **Site Map** (one of the menu options at the top of the page) for an overview of how the website is set up. There is also a **Help** page that you can access from the IPC's homepage at **www.ipc.on.ca**, as well as from many other sections of the website.

Mediation success stories

"Mediation success stories" is a regular column highlighting several of the recent appeals or privacy complaints that have been resolved through mediation.

Police, appellant worked together to resolve appeal

The Pembroke Police Service received a request under the *Municipal Freedom of Information and Protection of Privacy Act* for "the investigation notes … together with a copy of any documentation arising out of the investigation" regarding a missing deposit bag. The police denied access to the responsive records pursuant to section 8(2)(a) and 14(3)(b) of the *Act*. The requester (now the appellant) appealed the decision to the IPC.

During a background meeting with the mediator, the appellant's representative indicated that the freedom of information request was made in an effort to adduce written evidence that the appellant was no longer under investigation. The mediator set up a teleconference meeting with both parties so that they would have an opportunity to share their concerns directly with one another.

At the teleconference mediation session, the appellant's representative outlined his concerns and the police service indicated that though it was not prepared to revise its decision, it was prepared to prepare a letter advising that there was insufficient information to list the appellant as the lone suspect.

Though the appellant's representative did not get access to the records in dispute, he nonetheless was satisfied with the process and the police service's willingness to provide as much information as it deemed possible under the *Act*.

By working together to find solutions rather than as adversaries, the parties were able to agree on a mediated resolution that addressed their concerns.

Form created, policy being developed, after PHIPA complaint

The IPC received a complaint under the *Personal Health Information Protection Act* from an individual who had been denied a request she made to her former employer's occupational health department to correct her occupational health record. The employer is a health care facility.

The occupational health department had responded in writing to the complainant's request to correct her record. The response letter denied the request and indicated that the complainant's request letter would be added to the file.

The complaint proceeded to mediation at the IPC and the mediator had several telephone discussions with both parties.

The complainant indicated that the record involved was an entry made by an occupational health nurse in the complainant's occupational health record. The entry arose as a result of the complainant's visit to her employer's occupational health department, due to discomfort while at work. The complainant was of the view that the entry was incomplete and inaccurate and should be corrected to reflect that her discomfort was work related, possibly due to the physical requirements of her job. The complainant also indicated that in the facility's response to her request, no rationale was provided for denying the request.

The facility indicated that the entry reflected the nurse's recollection of the complainant's visit. Specifically, it was the nurse's practice to ask each employee with a concern if he or she felt the symptoms were work related, and, if so, to document that the concern was work related and provide the employee with a workplace occurrence report for completion. In this case, the complainant did not complete a workplace occurrence report. In addition, the facility indicated that the nurse would not be able to change the entry to reflect a possible diagnosis, as diagnosing was beyond the scope of nursing practice. The facility also indicated that there was no supporting documentation to warrant changing the entry.

The health care facility also indicated that, as a result of the complaint, it has developed a form to enable individuals to request a change in their personal health information and was in the process of developing a policy regarding the correction of personal health information. In addition, the facility's privacy manager suggested to the facility that she be notified if requests for correction of personal health information are received. And, the privacy manager advised the facility that requesters should be provided with written reasons in cases where corrections to personal health information are denied.

After further discussions with the mediator, the complainant agreed, in resolution of this complaint, to prepare a statement of disagreement and submit it to the facility for consideration. The facility confirmed in writing to the complainant that the statement was received, appended to the occupational health record and would be released whenever the file is released.

The day that the lights went out

Most people who live in southern Ontario remember exactly where they were in the summer of 2003 when the lights went out – after a failure in an American power grid linked to a number of states and Ontario sparked a massive blackout.

The blackout resulted in some lingering problems and gave rise to a number of access requests.

In this case, a requester wanted to know if there were any environmental concerns caused by the blackout. He made a request under the *Freedom of Information and Protection of Privacy Act* to the Ministry of the Environment for access to certain records.

The ministry responded that, after a thorough search through the files of its Investigations and Enforcement Branch, no records were located that were responsive to the request. The requester (now the appellant) appealed that decision to the IPC.

Continued on Page 12

Summaries

"Summaries" is a regular column highlighting significant orders and privacy investigations.

Order MO-2072
Appeal MA-040138-2
Toronto District School Board

This appeal involved a request under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) to the Toronto District School Board for access to a copy of the evaluation report prepared by the board with regard to its *request for proposals* (*RFP*) for the provision of information technology contract staff.

The board located one responsive record, a spreadsheet referred to as the "bid evaluation," a summary report evaluating the bids it received and considered. The bid evaluation consisted of several categories of pricing information, comprised of staff pay rates for various positions, margins, overtime rates, discounts and other fees drawn from the proposals submitted by the 24 affected parties in response to the RFP. The bid evaluation also contained information under the heading, "reasons for disqualification."

The board applied the third party information exemption in section 10(1) of the *Act* to deny the requester access to the record. The requester appealed the decision to the IPC, and the board and 10 of the affected parties submitted representations claiming that disclosure of the information at issue could reasonably be expected to result in one of the harms listed at section 10(1)(a) and 10(1)(c) of the *Act*. In support of their position, the board and the affected parties provided evidence as to what competitors would stand to gain from disclosure, including access to inside pricing and costing information, and the ability to underbid competitors. Adjudicator Bernard Morrow found that these sections did not apply, as the board and the affected parties had not met the harms test, and he ordered the release of the records in their entirety.

In reaching his decision, the adjudicator agreed that the decision whether to disclose specific bid information must be approached in a careful way in each case, considering the tests as developed over time by this office while appreciating the commercial realties of the RFP process and the nature of the industry in which it occurs [see Order MO-1888].

This decision is significant as it highlights that disclosure of pricing information does not automatically give rise to a reasonable expectation of harm.

In making his decision that the harms test under section 10(1) was not met, Adjudicator Morrow took into account the following factors:

- eight of the 24 affected parties consented to the release of their information;
- the information at issue was submitted by the affected parties more than two and a half years ago and there was little evidence to suggest that this information would be of any value to competitors today; and
- while price could play an important role in determining success in the bidding process, it was not the only assessment criteria that appeared in the bid evaluation, as the record also set out each affected party's overtime policy, price guarantee date, discount criteria and additional notes on particular points of interest in specific proposals.

Order PO-2494
PA-040327-1
Ministry of Community Safety and Correctional Services

This appeal involved a request made to the Ministry of Community Safety and Correctional Services under the *Freedom of Information and Protection of Privacy Act* for records relating to the appellant's firearms possession licence. The appellant had made the request following the execution of a search warrant at her residence by the OPP in a separate law enforcement matter unrelated to the request.

The responsive records included photographs and video tapes made during the search, OPP officers' notes, and internal OPP e-mails relating to the search and subsequent charges.

The ministry relied on section 49(a) (limitations on an individual's right to obtain own personal information), in conjunction with section 19 (solicitor-client privilege) of the *Act,* to withhold all of the records at issue. The ministry also relied on section 49(b) in conjunction with section 21 (personal privacy) to withhold some information.

The ministry submitted that because copies of the withheld records were included in the Crown brief maintained by Crown counsel for the purposes of a criminal prosecution, section 19 applied to the records. The ministry argued that any records in its possession that found their way into the Crown brief should automatically be seen as meeting the "prepared for Crown counsel in contemplation of or use in litigation" test described in section 19.

In rejecting the ministry's argument, Brian Beamish, Assistant Commissioner (Access), found that the records were prepared for investigative purposes to assist it in determining whether to lay criminal charges for possession of firearms. He found that this purpose was distinct from Crown counsel's use of copies of the records in order to decide whether or not to prosecute criminal charges and, if so, using the records to conduct the litigation. The Assistant Commissioner found that the fact that copies of the records found their way into the Crown brief does not alter the purpose for which the records were originally prepared and now maintained by the ministry.

In arriving at this decision, the Assistant Commissioner took into account the fact that investigative records

Continued on Page 12

Mediation Success Stories

CONTINUED FROM PAGE 10

During the mediation process, the mediator first contacted the appellant. The appellant acknowledged that the request letter to the ministry may not have been as clear as was intended. The letter did not include sufficient detail to help the ministry conduct a proper search.

The mediator suggested that a conference call be set up involving the appellant, the mediator and the ministry. During this conference call, the appellant was able to clarify his request and provide additional details. As a result of this discussion, the ministry agreed to conduct an additional search for records and expanded the search to include different departments.

The ministry located responsive records and granted access to the appellant. After reviewing the records, the appellant advised the mediator that he was satisfied with the records provided and that there was no need to pursue his appeal. The appellant was appreciative of the fact that the ministry had given him the opportunity at the teleconference to explain his request.

The conference call lasted less than half an hour and resulted in the appellant obtaining the information he was seeking. As a result of the direct communication between the appellant and the ministry, this appeal was successfully resolved.

Summaries

CONTINUED FROM PAGE 11

are protected by the law enforcement provisions of section 14 of the *Act*. He also found that to accept the ministry's argument would be to extend the ambit of section 19 to almost any investigative record created by the police. The Assistant Commissioner was of the view that this would undermine the access to information purposes of the *Act*. He stated that if he found that the privilege exemption applied in the circumstances of this appeal, the result could be that records that police across Ontario now routinely disclose would be withheld in the future, thereby fundamentally altering a long-standing disclosure practice.

He also found that some of the information the ministry withheld under sections 49(b)/21 was exempt, while some was not exempt.

Accordingly, Assistant Commissioner Beamish ordered the ministry to disclose the responsive records to the appellant, with the exception of the exempt personal information.

Order PO-2500
Appeal PA-030106-5
Ministry of the Environment

The Ministry of the Environment received a request for all information produced within the ministry or received by the ministry associated with any environmental reports involving the Bruce Nuclear Power Development in Tiverton, Ontario.

This appeal is the fifth of a series of appeals to the IPC arising from the same request. The history of the first four appeals is described in detail in Order PO-2243, which resolved Appeal PA-030106-4. In response to that order, the ministry decided to disclose a portion of the responsive records and to deny access to other records, in whole or in part, pursuant to the exemptions at sections 14(1)(i) (security of a building), 16 (national security), 17(1)(a) and (c) (third party information), 19 (solicitor-client privilege), 21(1) (personal privacy) and 22(a) (publicly available information) of *the Freedom of Information and Protection of Privacy Act (*the *Act)*.

In her appeal letter, the appellant raises the possible application of the "public interest override" at section 23 to the information contained in the records.

The ministry's representations respecting section 16 focus primarily on its concerns about the potential for violent attacks against the Bruce nuclear facilities. The ministry also makes it clear that its concerns arise from the fact that, once information is disclosed, it is in the public domain. The ministry included in its representations advice it received from the local police force concerning the impact of disclosing the records for which it claimed this exemption.

Adjudicator John Higgins points out that the governments of Canada and the United States have both taken steps to minimize the risk of attacks intended to harm their populations in the wake of the terrorist attacks of September 11, 2001 with legislative action, for example the U.S. *Patriot Act* and Canada's *Anti-Terrorism Act*. Clearly, in the view of the adjudicator, this risk extends to facilities such as nuclear power plants.

The adjudicator, having reviewed the records and the submissions of the parties, found that the disclosure of records or parts of records setting out detailed technical information about the nuclear and related operations of the Bruce facility could reasonably be expected to "… prejudice the defence of Canada … or be injurious to the detection, prevention or suppression of espionage, sabotage or terrorism" and was, therefore exempt under section 16.

Adjudicator Higgins protected further records under the solicitor-client privilege exemption, while the remainder of the records, for which other exemptions were claimed, were ordered released.

IPC
PERSPECTIVES
is published by the **Office of the Information and Privacy Commissioner/Ontario**.

If you have any comments regarding this newsletter, wish to advise of a change of address, or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Cette publication, intitulée «Perspectives», est également disponible en français.

30% recycled paper

ISSN 1188-2999