Yukon Information & Privacy Commissioner

Best Practice: Responding to a Privacy Breach

Introduction

The *Access to Information and Protection of Privacy Act* (ATIPP Act or Act) has a dual purpose: to "make public bodies more accountable to the public" and "to protect personal privacy" (section 1). The Act balances the right of access to government records with the protection of privacy. It provides a right of access to records in the custody or under the control of public bodies. Limited exceptions to the right of access are specifically set out in the Act.

The Yukon's Information and Privacy Commissioner (IPC) has issued a series of Best Practices to assist in understanding the obligations of the ATIPP Act and the expectations of the IPC. The Best Practices are designed to help ensure responses to access requests are based on fair and consistent administrative decisions and to ensure that individuals' privacy is protected.

This Best Practice is designed to provide guidance to public bodies to develop a comprehensive and consistent approach for responding to privacy breaches.

What Is Personal Information?

All *personal information* collected by a public body must be kept private unless the public body has the authority under the ATIPP Act to use and or disclose it. Personal information has a broad definition in the privacy world; simply because it is easy to find a person's address or telephone number or sex on the internet or in the phone book does not mean it is not *personal information*. Personal Information is defined in the ATIPP Act (section 3) as recorded information about an identifiable individual including:

- the individual's name, address, or telephone number;
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
- the individual's age, sex, sexual orientation, marital status, or family status;
- an identifying number, symbol, or other particular assigned to the individual;

- the individual's fingerprints, blood type, or inheritable characteristics;
- information about the individual's health care history, including a physical or mental disability;
- information about the individual's educational, financial, criminal, or employment history;
- anyone else's opinions about the individual, and
- the individual's personal views or opinions, except if they are about someone else.

What is a Privacy Breach?

A privacy breach is not defined in the ATIPP Act. A privacy breach occurs when there is unauthorized collection, use or disclosure of personal information. The most common privacy breach happens when personal information of an individual, in the hands of a public body, is mistakenly disclosed, lost or stolen. For example, when a laptop or memory stick containing personal information is stolen or personal information is mistakenly emailed to the wrong person. A privacy breach may also be the consequence of faulty business procedure or operational breakdown.

Establishing a Privacy Breach Protocol

All public bodies should take the time to develop a privacy management framework. A privacy management framework outlines formal practices and safeguards to efficiently process privacy issues arising from operations whereby risks can be considered and mitigated. Privacy issues, including privacy breaches, may be prevented with the creation and compliance with a well structured privacy management framework. A privacy breach protocol, to assist public bodies in effectively responding to a privacy breach, is an essential element of a privacy management framework.

The Role of the IPC in Responding to a Privacy Breach

While notifying and/ or reporting a privacy breach to the IPC is not mandatory, the IPC has expertise and experience to assist a public body in professionally and efficiently responding to a privacy breach. Notifying the IPC will not immediately result in an investigation of the matter. The intervention of the IPC will depend entirely on the circumstances of a particular matter and how it is being managed by the public body. Documented investigations completed by the public body according to its' privacy breach protocol will enable the IPC to understand what has occurred and provide meaningful and timely assistance. A Privacy Breach Checklist is included here to help a public body review and communicate the circumstances surrounding a privacy breach to the IPC.

Proactively notifying the IPC as soon as the privacy breach is discovered puts the public body in control of how and when the IPC learns of the privacy breach. Notifying the IPC may, in some cases, enhance the public's understanding of the incident and confidence in the public body.

No matter how the IPC becomes aware of a privacy breach, she has the authority to investigate the matter.

Four Key Steps in Responding to a Privacy Breach or Suspected Breach:

1) breach containment and preliminary assessment;
2) notification;
3) others to contact; and
4) prevention.

Every potential privacy breach must be addressed immediately to determine what has occurred and assess the scope of the breach. Steps 1, 2 and 3 should be undertaken either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to appropriately respond to a privacy breach should be made on a case-by-case basis.

STEP 1: Breach Containment and Preliminary Assessment

Take immediate common sense steps to limit the breach:

- Immediately contain the breach. For example, stop the unauthorized practice, recover the original personal information subject to the breach, ensure no copies of the personal informtion were made or retained, shut down the system that was breache*d*, revoke or change computer access codes, and/ or correct weaknesses in physical or electronic security.
- Designate an appropriate individual within the public body with requisite knowledge and training to lead the response to the privacy breach including conducting the initial investigation.
- Determine the need to assemble a team to assist in responding to the privacy breach which could include appropriate public representatives.
- Determine who needs to be made aware of the incident internally, and externally, at this preliminary stage. Notifying the IPC at this stage will help the public body respond in the most effective manner.

- If the breach appears to involve theft or other criminal activity, notify the police.
- Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.

STEP 2: Notification

Notification of a privacy breach can help mitigate possible damage and has the potential to benefit both the public body and the individuals affected by a breach. If a privacy breach creates a risk of harm to someone, those affected should be notified. Prompt and proper notification can help individuals mitigate the damage by taking steps to protect themselves. The challenge is to determine when and what type of notice should be given. This will need to be done, on a case by case basis, by taking into account all of the circumstances of the matter. The IPC can assist with determining whether notification is required and if so what form it should take.

The key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been breached. Each decision of whether to notify needs to consider the interests of the individual whose personal privacy was breached and not just from the perspective of the public body.

Deciding about Notification: What is the Risk ?

- What is the context of the personal information involved? *For example, a list of customers on a newspaper carrier's route may not be sensitive. However, the same information about customers who have requested service interruption while on vacation may be more sensitive. Similarly, publicly available information such as that found in a public telephone directory may be less sensitive.*
- What was the extent of the unauthorized collection, use or disclosure of personal information? What is the number and nature of likely recipients and the risk of further access, use or disclosure? Is there a risk of disclosure using mass media or online?
- Who is the recipient of the information? Is there any relationship between the unauthorized recipient(s) and the data subject? *For example, was the disclosure to an unknown party or to a party suspected of being involved in criminal*

activity where there is a potential risk of misuse? Or was the recipient a trusted, known entity or person that would reasonably be expected to return the information without disclosing or using it?

- Who is affected by the breach: employees, contractors, public, clients, service providers, other public bodies?
- How sensitive is the personal information? *Generally, the more sensitive the information, the higher the risk of harm to individuals. Some personal information is more sensitive than others (e.g., health information, government-issued pieces of identification such as social insurance numbers, driver's licence and health care numbers, and financial account numbers such as credit or debit card numbers that could be used in combination for identity theft). A combination of personal information is typically more sensitive than a single piece of personal information. However, sensitivity alone is not the only criteria in assessing the risk - foreseeable harm to the individual is also important.*
- Can the personal information be used for fraudulent or otherwise harmful purposes including security risks, identity theft, loss of business or employment opportunities, or humiliation, damage to reputation or relationships? *The combination of certain types of sensitive personal information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.*
- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?
- Is there a risk of ongoing breaches or further exposure of the information?
- Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Has the personal information been recovered?
- What steps have already been taken to mitigate the harm?
- Is this a systemic problem or an isolated incident?
- Could harms such as risk to public health or risk to public safety be a result of the privacy breach?
- Could harms such as loss of trust in the public body, loss of assets, financial exposure or legal proceedings result from the privacy breach?
- What are the applicable legal and contractual obligations to notify an individual when a privacy breach occurs?

Consider the individual:

- What is the risk of harm to the individual?
- Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's

name and address together with government-issued identification numbers or date of birth)?
- Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?
- Is there a risk of humiliation or damage to the individual's reputation (e.g., when the information lost includes mental health, medical or disciplinary records)?
- What is the ability of the individual to avoid or mitigate possible harm?

When, How and Who Should Notify

- **When to notify:** Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, check with those authorities about the timing of the notification to ensure that the investigation is not compromised.
- **How to notify:** The preferred method of notification is direct – by phone, letter, email or in person – to the affected individual(s). Indirect notification such as website information, posted notices and media should generally only be used where direct notification could cause further harm, the cost is prohibitive or the contact information for affected individual(s) is not known. Using multiple methods of notification in certain cases may be appropriate. Consider whether the method of notification might increase the risk of harm (example: by alerting the person who stole the laptop of the value of the information on the computer).
- **Who should notify:** Typically, the public body that has a direct relationship with the customer, client or employee should notify the affected individual(s), including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information. However, there may be circumstances where notification by a third party is more appropriate. For example, in the event of a breach by a retail merchant of credit card information, the credit card issuer may be involved in providing the notice since the merchant may not have the necessary contact information.

Content of Notification

Make sure that any notification does not contain unnecessary personal information so as to avoid possible further unauthorized disclosure.

- Include information about the incident and its timing in general terms.
- Include a description of the personal information involved in the breach.
- Include a general account of what the public body has done to control or reduce the harm.
- Explain what the public body will do to assist individual(s) and what steps they can take to avoid or reduce the risk of harm or to further protect themselves. Possible actions include arranging for credit monitoring or other fraud prevention tools, providing information on how to change a social insurance number (SIN), personal health card or driver's licence number.
- Include sources of information designed to assist individuals in protecting against identity theft (e.g., online guidance on the Office of the Privacy Commissioner's website http://www.priv.gc.ca/keyIssues/ki-qc/mc-ki-idt_e.cfm and Industry Canada website at http://strategis.ic.gc.ca/epic/site/oca-bc.nsf/en/h_ca02226e.html);
- Provide contact information of a department or individual within the public body who can answer questions or provide further information;
- If applicable, indicate whether the public body has notified the IPC and that the IPC is aware of the situation;
- Include additional contact information for the individual to address any privacy concerns to the public body; and
- Include contact information for the IPC.

STEP 3: Others to Contact

Before contacting other organizations or offices, make sure that contact is in complaince with ATIPP or other privacy laws:

- The IPC should be notified in a timely manner regarding any privacy breach and should be notified immediately in situations of a material privacy breach;
- Police if theft or other crime is suspected;
- Insurers or others if required by contractual obligations;
- Professional or other regulatory bodies if professional or regulatory standards require notification of these bodies;
- Credit card companies, financial institutions or credit reporting agencies if their assistance is necessary for contacting individuals or assisting with mitigating harm;
- Other internal or external parties not already notified;
- Third party contractors or other parties who may be impacted;

- Internal business units not previously advised of the privacy breach, e.g., government relations, communications and media relations, senior management, etc.; and/or
- union or other employee bargaining units.

STEP 4: Prevention of Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, public bodies need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach and whether it was a systemic breach or an isolated instance.

Develop a Prevention Plan that may include the following:

- a security audit of both physical and technical security;
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (e.g., security policies, record retention and collection policies, etc.);
- a review of employee training practices; and
- a review of service delivery partners (e.g., dealers, retailers, etc.).

The resulting plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.