A Policy is Not Enough:

It Must be Reflected in Concrete Practices

September 2012

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Information and Privacy Commissioner,
Ontario, Canada

TABLE OF CONTENTS

Introduction

A privacy policy cannot, by itself, protect personal information[1] held by an organization. Privacy policies that are not reflected in actual practice through strong implementation, training, and auditing will fail to safeguard personal information against privacy risks. But if we return to the true meaning of "policy," we will be reminded that it was always intended to be rooted in action. *The Concise Oxford Dictionary* defines policy as: "a course, or general plan of action adopted or proposed..."

Privacy and data protection policies must be operationalized throughout the activities of an organization. Deeply-embedded policies and procedures not only help to establish an organizational culture of respect for privacy, but will ensure that the necessary protections are actualized. *Privacy by Design* (*PbD*) is an example of a proactive approach to privacy, one that provides both a framework and a methodology. *PbD* is premised on the notion that privacy is best assured when strategically interwoven into all business processes and practices (*e.g.*, work processes, management structures, physical spaces, information technology and networked infrastructure). Based on a set of 7 Foundational Principles, *PbD* offers a flexible and technology-neutral vehicle for engaging with privacy issues, and for resolving them in ways that support multiple outcomes in a positive-sum, win-win scenario as opposed to a zero-sum, either/or scenario. The Principles are as follows:

1. *Proactive* not Reactive; *Preventative* not Remedial
2. Privacy as the *Default Setting*
3. Privacy *Embedded* into Design
4. Full Functionality – *Positive-Sum*, not Zero-Sum
5. End-to-End Security – *Full Lifecycle Protection*
6. *Visibility* and *Transparency* – Keep it *Open*
7. *Respect* for User Privacy – Keep it *User-Centric*

The aim of this proactive approach is to reduce the risk of privacy harm from arising in the first place, ideally preventing it entirely, while preserving a commitment to functionality.

Privacy leaders from around the world have endorsed the importance of *PbD*.[2] At the 32nd International Conference of Data Protection and Privacy Commissioners in 2010, *Privacy by Design* was unanimously passed and adopted as an International

1 Throughout this paper "personal information" includes "personal health information."

2 These individuals include: Peter Hustinx, European Data Protection Supervisor; Viviane Reding, Vice President, Justice, Fundamental Rights and Citizenship, European Commission; and John Leibowitz, Chairman, US Federal Trade Commission.

framework for protecting privacy.[3] Considered a "landmark resolution," *Privacy by Design* was recognized as an "essential component of fundamental privacy protection."

Even the most forward-looking privacy and data protection policies must be operationalized within an organization – not by chance, but by design – in order to be effective. Commitment to privacy and data protection starts with an organization-wide privacy framework that sets forth senior management's strong support for privacy protection. Of course, strong policies are necessary, but insufficient on their own to address privacy risks; implementation and strong oversight are also essential to move from policy to practice.

In this paper, I set out a series of steps that organizations should consider implementing in order to effectively translate their privacy policies into privacy practices:

1. Implement a privacy policy that reflects the privacy needs and risks of the organization and consider conducting an effective Privacy Impact Assessment;

2. Link each requirement within the policy to a concrete, actionable item – operational processes, controls and/or procedures, translating each policy item into a specific practice that must be executed;

3. Demonstrate how each practice item will actually be implemented;

4. Develop and conduct privacy education and awareness training programs to ensure that all employees understand the policies/practices required, as well as the obligations they impose;

5. Designate a central "go to" person for privacy-related queries within the organization;

6. Verify both employee and organizational execution of privacy policies and operational processes and procedures; and

7. Proactively prepare for a potential privacy breach by establishing a data breach protocol to effectively manage a breach.

Given the significant differences that exist among organizations, there is no "one-size-fits-all" approach to reflecting policy in practice. Rather, this paper is intended to set forth practical guidance and examples of steps that an organization should be taking to ensure that its policy is actually implemented through a definite course of action, thereby preventing privacy breaches from arising.

3 International Conference of Data Protection and Privacy Commissioners (2010). *Privacy by Design* Resolution, adopted at Jerusalem, Israel, October 27-29, 2010. At http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf.

Step 1: Implement an Appropriate Privacy Policy and Consider Conducting a Privacy Impact Assessment

While implementing a privacy policy is an important step towards protecting personal information, it needs to be done right. Simply having a generic privacy policy, which does not consider the particular challenges of a given organization, is not sufficient. Each organization should assess potential privacy risks and ensure that it has an *appropriate* and easy-to-understand policy based on the size and structure of the organization and the privacy challenges that it faces.

Each organization, regardless of its size, should develop and implement an overarching privacy policy that applies to all aspects of its information management processes (*i.e.*, the collection, use, retention, disclosure, and destruction of personal information). This policy should be consistent with industry standards, as well as any orders, guidelines, fact sheets, and best practices issued by my Office. To gain a sense of the current privacy status of an organization as measured against best practices, one should consider completing a privacy maturity model.[4] This can suggest the direction that an organization should take to achieve a mature privacy approach.

For organizations holding sensitive personal information or large amounts of personal information, I would also recommend that a comprehensive Privacy Impact Assessment (PIA) of the organization's data holdings and processes be undertaken. PIAs and other risk assessment tools (such as a security threat assessment) can assist in determining the vulnerabilities that exist within an organization, thereby enabling it to develop and implement a privacy policy that addresses a broad range of issues.

A PIA generally includes a description of the:

- Data holding, information system, technology or program at issue;
- Nature and type of personal information collected, used, or disclosed (or that is proposed to be collected, used, or disclosed);
- Sources of the personal information;
- Primary purpose(s) for which the personal information is being collected, used, or disclosed (or, that is proposed to be collected, used, or disclosed);
- Reason that the personal information is required for the purpose(s) identified;
- Flows of the personal information – both direct and indirect;

4 See the American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants Privacy Maturity Model at http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/pages/aicpacicaprivacymaturitymodel.aspx.

- Statutory authority for each collection, use, and disclosure of personal information identified;
- Limitations imposed on the collection, use, and disclosure of the personal information;
- Whether or not the personal information is or will be linked to other information;
- Retention period for the records of personal information collected;
- Secure manner in which the records of personal information are (or will be) retained, transferred, and disposed of;
- Administrative, technical, and physical safeguards implemented or proposed to be implemented to protect the personal information collected;
- Functionality for logging access, use, modification, and disclosure of the personal information;
- Access controls and audit logs implemented to restrict unauthorized use or disclosure;
- Risks to the privacy of individuals whose personal information is (or will be) part of the data holding, information system, technology, or program, and an assessment of these risks; and
- Recommendations to eliminate or reduce any privacy risks identified.

It is important to remember that where a PIA has been completed, it should be reviewed on an ongoing basis in order to ensure that it continues to be accurate, up to date, and consistent with the organization's information practices.

A helpful example of a PIA framework is provided in *A Foundational Framework for a PbD-PIA* by Anita Fineberg and Pat Jeselon.[5] The framework utilizes the 7 Foundational Principles of *PbD* to structure the PIA. These Principles are discussed as they apply in three areas: (i) information technology; (ii) accountable business processes; and (iii) physical design and networked infrastructure. An organization could customize this framework to create a PIA that meets its own privacy and organizational needs.

In addition to conducting a PIA, there is also a need for regular[6] reviews of organizational privacy policies, procedures, and practices to determine whether amendments and/or new policies, procedures, and practices are required. In undertaking these reviews, an organization should consider:

5 Fineberg, A. and Jeselon, P. (2011). *A Foundational Framework for a PbD – PIA* at http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf.

6 As the default benchmark, I recommend an annual review that may vary, depending upon the specific factors in each organization.

- Any orders, guidelines, fact sheets and best practices issued by my office;
- Evolving industry privacy standards and best practices, technological advancements, and amendments to relevant legislation;
- Any recommendations arising from privacy and security audits, PIAs, and investigations into privacy complaints, privacy breaches, and information security breaches; and
- Whether the privacy policies and procedures of the organization continue to be consistent with its actual practices, and whether there is consistency between and among the privacy policies and procedures implemented.

Step 2: Link Requirements in Privacy Policy to Concrete Action Items, Procedures, and Controls

While having a strong privacy policy is important, it is only the first step. An organization, and more specifically senior management, needs to develop and implement a method of translating the policy into a series of specific practices or action items that must be executed within the organization's operations. For every requirement set out in the policy, the organization should consider how it can most effectively achieve it through concrete, actionable items. These actionable items must clearly identify who is responsible for executing them and how each requirement will be met.

For example, if an organization's privacy policy forbids the use of unencrypted USB memory keys, the organization would need to consider how to operationalize this requirement by building in strong encryption, by default. Two possible solutions would be to require the exclusive purchase/use of hardware encrypting "secure" USB drives, or to centrally manage end-point encryption by default, at the enterprise level. The organization should also consider best practice options, such as establishing secure remote workstations[7] (whether permanent or portable). These action items will translate the actual privacy policy into concrete operational practice.

Step 3: Demonstrate How Each Practice Item will be Implemented

In order to effectively implement change within an organization, there needs to be strong "buy in" from the top. Senior management needs to be aware, not only of the organization's privacy policy, but also how that policy is going to be operationalized through concrete actionable items. For example, if a practice item

7 See *Stop. Think. Protect.* at http://www.ipc.on.ca/English/Privacy/Stop-Think-Protect-/ and *Safeguarding Privacy in a Mobile Workplace: Protect the information you keep on your laptops, cellphones and PDAs* at http://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=628.

calls for the use of hardware encrypting "secure" USB drives, those individuals responsible for implementation would be required to demonstrate to management how this outcome will be accomplished.

To create a "privacy smart" leadership team, it is imperative that the action items be explained and vetted through senior management to ensure their operational success. The benefits of such an approach are twofold: (i) informing management of practical privacy initiatives; and (ii) providing an opportunity for the organization's management to give feedback and suggestions on these vital organizational operations.

Step 4: Develop a Privacy Education and Awareness Training Program

In this modern digital world, employees need to understand data privacy and how to manage sensitive information. While such awareness and training will help to achieve end-to-end security – an important *PbD* principle – it is also key to enabling a broader, proactive approach to privacy. Ensuring that employees are aware of what is expected of them in this privacy domain helps to build an organizational culture that values privacy and strives to protect personal information. Proper training enables employees to internalize this goal of privacy protection and creates a heightened awareness of potential privacy issues. Technology and security can only do so much; "privacy smart" employees are essential to effectively managing the organization's personal information.

All employees (including the senior management team, departmental managers, and frontline staff) should attend an initial privacy orientation as well as regular continuing privacy training. Where feasible, I also recommend that organizations develop privacy education/training procedures that identify the timeframe, frequency, and content of both the initial orientation and ongoing privacy training, to ensure that training remains formalized and standardized within the organization.

(a) Initial Training

An initial privacy orientation session should be provided when an employee commences work at the organization. In addition to introducing the employee to the organization's privacy protocols, training should explain how and why data protection is an important part of the employee's work. This training could include:

- A description of the status of the organization (*e.g.*, an institution under the *Freedom of Information and Protection of Privacy Act*) and the duties and responsibilities that arise as a result of this status;
- A description of the nature of the personal information collected, and from whom this information is typically collected;

- An explanation of the purposes for which personal information is collected and used, and how this collection and use is permitted by relevant legislation;
- Limitations placed on access to, and use of, personal information by employees;
- An explanation of when and how to effectively use encryption with the handling of personal information. This should be preceded by an explanation of the reasons why encryption should be used;
- A description of the procedure that must be followed in the event that an employee is requested to disclose personal information;
- An overview of the privacy policies, procedures, and practices that have been implemented by the organization and the obligations arising from these policies, procedures, and practices;
- The consequences of a breach of the privacy policies, procedures, and practices implemented;
- An explanation of the privacy program, including the key activities of the program and the employee(s) that have been delegated day-to-day authority to manage the privacy program;
- Safeguards that have been implemented at the organization to protect personal information against theft, loss, and unauthorized use or disclosure;
- The duties and responsibilities of employees in implementing safeguards that have been put in place by the organization;
- A discussion of the nature, purpose, and key provisions of any confidentiality agreement that employees must execute as a condition of employment; and
- An explanation of the privacy breach protocol and the duties and responsibilities imposed on employees in identifying, reporting, containing, and participating in the investigation and remediation of privacy breaches.

Employee privacy orientation should also include a review of how the organization will monitor compliance with its policies and procedures, as well as an explanation of the consequences of breaching these obligations.

(b) Ongoing Training

In addition to an initial orientation, both employees and management need to be reminded of existing privacy policies and procedures. Ongoing privacy education and awareness training will provide employees with ready access to the information they need to recognize and properly handle personal information. It also provides the organization with an opportunity to address any new privacy

policies, procedures, and practices, and any notable amendments required. These training sessions should integrate any recommendations with respect to privacy training made in PIAs, privacy audits, and investigations of privacy breaches and privacy complaints.

Similar to the initial privacy orientation, ongoing privacy training should become a routine affair. In addition, I recommend that employees confirm, annually, that they have reviewed all relevant privacy policies and completed any necessary privacy training. Employees may verify completion of a training course by providing proof of training, such as a dated certificate, electronic update, or similar forms of confirmation.

(c) Methods of Training

Choosing an appropriate mix of effective training methods is crucial to empowering privacy-conscious employees. Different awareness methods and educational tools should be utilized, depending on the target audience, the privacy issues involved, and the size of the organization, among other factors. A September 2011 paper co-authored by my Office and IBM provides an excellent case study of how IBM has integrated various educational techniques into the company's workplace privacy training.[8]

One conventional method of employee training is instructor-led presentations conducted by internal experts or external training providers. For example, Service Alberta offers five different instructor-led privacy training courses for employees in the Alberta public service.[9]

A further method that can be utilized to educate employees on privacy issues is individual, self-paced online tutorials. These tutorials often guide the user through online modules of informative click-through presentations that are followed by a quiz. For example, the Saskatchewan provincial government has set up an online access and privacy course for local authorities in the province.[10]

Many online training modules incorporate tests throughout the session to keep users engaged and motivated during the tutorial. Quizzes and tests can be conducted after training is complete to evaluate whether the training successfully conveyed the organization's policies and procedures to employees. The benefits of such evaluation techniques are two fold: (i) helping employees identify areas of imperfect knowledge which require further review; and (ii) (assuming the results of the tests are collected by the organization) allowing the organization to identify topics in its privacy training which are not being effectively conveyed to employees, so that those sections can be revised to better reach the intended audience.

---

8 *Privacy by Design*: From Policy to Practice. (2011). At http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1113.

9 Service Alberta. Training for public bodies at: http://www.servicealberta.ca/foip/training/instructorled-training.cfm.

10 Government of Saskatchewan. Ministry of Justice and Attorney General. Access and Privacy Course for Saskatchewan Local Authorities. At http://www.justice.gov.sk.ca/PrivacyLA/html/curriculum000F1F652B9D0F24C80E020500000044.htm ; See also online training offered by Service Alberta at http://www.servicealberta.ca/foip/training/online-training.cfm.

Whether through instructor-led sessions or online multimedia learning, I recommend that employee privacy education incorporate role-playing exercises and/or what-if scenarios. Role-based training helps to ensure that employees understand how to apply the privacy policies, procedures, and practices in their day-to-day employment responsibilities. These scenarios can also integrate into the training, examples of past employee errors, and demonstrate how the errors could have been avoided. Research has found that incorporating error-based training leads to improved judgment and adaptive thinking, as compared to error-free training.[11]

Regardless of the type of training selected, it is helpful to provide employees with manuals, guides, checklists, or charts to retain as reference materials after training is complete. For example, Memorial University provides a Privacy Training Manual and Tips and Guidelines Sheet as part of privacy training sessions of employees.[12] Additionally, my office has produced several informative guidance and best practice documents.

- ***Privacy Breach Protocol Guidelines for Government Organizations***
  http://www.ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=292

- ***Privacy by Design: From Policy to Practice***
  http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1113

- ***The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users***
  http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1040

- ***Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default***
  http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=946

- ***Stop.Think.Protect.***
  http://www.ipc.on.ca/English/Privacy/Stop-Think-Protect-/

- ***Breach Notification Assessment Tool***
  http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=581

11 Joung, W., Hesketh, B., Neal, A. (2006). Using "War Stories" to Train for Adaptive Performance: Is it Better to Learn from Errors or Success? *Applied Psychology: An International Review*, 55, 282-302.

12 Memorial University. Information Access and Privacy Protection. Privacy Training at http://www.mun.ca/iapp/privacy/training.php.

- ***Safeguarding Privacy in a Mobile Workplace: Protect the information you keep on your laptops, cellphones and PDAs***
  http://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=628

- ***Privacy Diagnostic Tool (PDT) Workbook***
  http://www.ipc.on.ca/English/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=293

(d) Other Awareness Methods

While employee training is vital to privacy awareness, other mechanisms should be implemented by the organization to foster a culture of privacy and to raise awareness of the privacy program and the privacy policies, procedures, and practices implemented. This may include adopting new communication strategies, such as screensavers and pop-ups with notices and reminders about privacy. Organizations can also create a log-on message, asking employees to acknowledge that their access is appropriate, and reminding them about random audit programs.

Visible executive-level commitment to privacy also helps to incorporate these values into an organization's culture, which leads to the successful implementation of the privacy policies. For example, senior management could use internal "e-mail blasts," newsletters, and staff meetings to relay privacy messages to employees on a regular basis. By integrating privacy systematically throughout the organization's materials, beyond the initial training, privacy is further entrenched into the workplace, ideally becoming the organization's default setting.

Step 5: Designate a Privacy "Go to" Person

Even the best employee training will not answer all privacy-related challenges that an organization may face in its day-to-day operations. As a result, it is key that every organization has a central "go to" person (or group) who can answer internal questions about privacy requirements or the implications of particular practices on privacy. This privacy specialist should have the expertise and authority to address privacy concerns by either providing a solution to the problem or directing employees to the appropriate resource. Additionally, in many organizations, it makes sense for this individual to be responsible for responding to privacy breaches and conducting any related investigations. Organizations should also have a backup "go to" person to assist employees in situations where the primary "go to" person is unavailable.

It is important that the privacy specialist's mandate and role is understood by staff and management throughout the organization. Further, the individual should be easily accessible to other employees so that he/she is able to act as a valuable resource within the organization. In larger organizations (or smaller ones with significant privacy challenges), I would advocate in favour of establishing a senior

management-level privacy specialist position (*e.g.*, a "Chief Privacy Officer") to oversee and be accountable for all privacy-related concerns at the organization. The senior privacy specialist should have access to other senior employees and directors, as well as the authority to ensure that projects and practices do not proceed where significant privacy and security implications have not been satisfactorily addressed.

In smaller organizations, it may not always be practical to create an employment position that is devoted solely to managing privacy concerns within the organization. However, there still needs to be a "go to" person at the organization who is knowledgeable and responsible for privacy-related issues. For example, these duties could be assigned to the head of such an organization or (where applicable) to the organization's Freedom of Information and Privacy Coordinator.

Step 6: Trust – but Verify Execution

An organization's responsibilities do not end with developing appropriate privacy policies and educating its staff about those policies. Beyond education and training, organizations must ensure that policies are made actionable. There must also be processes and procedures in place to verify that employees are complying with the organization's privacy policies. There are various methods, both formal and informal, that organizations can and should be using to verify compliance. One should never assume that policies are being met – trust, but verify.

(a) Formal Privacy Audits

One effective method of verifying compliance and ensuring that policies are executed is a comprehensive privacy audit of the organization. The general utility of privacy audits has been recognized by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA), who have jointly published their *Generally Accepted Privacy Principles (GAPP) – A Global Privacy Framework* (the *GAPP Privacy Framework*).[13] My Office was consulted heavily on the development of the GAPP.

Mandatory, organization-wide privacy audits help to ensure that an organization is operating properly with respect to privacy, and could help to reduce the risk of a privacy breach. In doing so, audits assist in validating an organization's privacy practices and ensuring the rigour of those practices, by identifying and addressing the gaps, and contributing to public confidence and trust.

Similar to privacy policies, audits must also be tailored to the organization's specific structure and the privacy issues involved. For example, in provincial ministries which collect, use, and disclose large amounts of personal information, an annual

13 The *GAPP Privacy Framework* was developed to assist organizations in identifying and managing privacy risks and serves as an excellent basis for conducting independent audits. The *GAPP Privacy Framework* is available from the CICA's website at: http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/gen-accepted-privacy-principles/item61833.pdf.

privacy audit by an independent third party may be appropriate. In contrast, smaller organizations, which handle minimal amounts of personal information, need not necessarily undertake such measures.

As a general best practice, I recommend that organizations verify compliance with their privacy policies, procedures, and practices, including through random audits of individual employees who have access to personal information held at the organization. An organization should set out in writing the types of privacy audits that are required, and how the audits are to be conducted. The policy and procedures for such audits should set out:

- Who is responsible for conducting the privacy audit;
- The purposes of the privacy audit;
- The criteria that should be considered in selecting the subject matter of the audit;
- The nature and scope of the privacy audit (*i.e.,* document reviews, interviews, site visits and/or inspections);
- Whether or not notification of the audit will be provided and, if so, the nature and content of the notification and to whom the notification must be provided;
- The frequency with which – and the circumstances in which – each privacy audit is required to be conducted. In this regard, the policy and procedures should require a privacy audit schedule to be developed, and should identify the individuals responsible for developing the privacy audit schedule;
- The nature of the documentation that must be completed, provided and/or executed at the conclusion of the privacy audit; and
- The manner and format in which the findings of privacy audits will be communicated, including the recommendations arising from the audits and the status of addressing the recommendations. This should include the person responsible for communicating the findings, the mechanism and format for communicating the findings, the timeframe within which this must occur, and to whom the findings will be communicated, including the head of the organization.

Records of the results of privacy audits should be maintained for future review. These records should include the recommendations arising from each audit and should track whether each recommendation was or is expected to be addressed, when it was or is expected to be addressed, and the manner in which it was or is expected to be addressed.

(b) Informal Audits

While, in many circumstances, a formal privacy audit is an important tool for verifying compliance, organizations should also consider less formal methods of verification. Organizations should seek to identify potential privacy concerns proactively, and not simply wait for those concerns to be identified through a formal audit process. For example, organizations could ask their information technology departments to perform unscheduled checks of mobile devices such as smartphones, USB memory keys, and laptop computers, to ensure that the devices have appropriate encryption and password protections.

(c) Appropriate Management Oversight

The role of management does not end with developing a privacy policy, ensuring that it is reflected in actual practice, and having the policy communicated to staff. Proper privacy protection requires the "buy in" of all employees, from all levels of the organization!

For highly sensitive personal information, organizations may consider requiring direct oversight by managers and/or senior staff of certain processes to ensure that privacy policies and procedures are being executed. For example, where sensitive or large amounts of personal information is to be sent to external sources as an attachment to an email message, it may be prudent for a senior staff member to review the email, prior to it being sent, to ensure that the file containing the personal information is in encrypted format.

Step 7: Prepare for a Possible Privacy Breach – Establish a Data Breach Protocol

It is increasingly important that organizations of all sizes be prepared to react to data security incidents, such as a privacy breach. A privacy breach occurs when personal information is collected, retained, used, or disclosed in ways that are not authorized. Among the most common breaches of personal privacy is the unauthorized disclosure of personal information. The causes of such incidents range from malicious activities to inadvertent lapses in the people or processes handling personal data. For example, personal information may be lost (a file is misplaced within an organization), stolen (USB memory keys are prime examples), or inadvertently disclosed through human error (a letter addressed to Person A is actually mailed to Person B). Whenever and wherever these things happen, and for whatever reasons, a disciplined and immediate response is vital in order to address the situation in a manner that protects individuals, meets regulators' expectations, and ultimately preserves the reputation of the affected organization.

When a privacy breach or suspected breach occurs, it is imperative that the organization react both quickly and effectively to manage the situation. As a result, I strongly advocate that organizations develop and implement protocols to address the identification, reporting, containment, notification, investigation,

and remediation of privacy breaches. All employees need to know what to do and who to notify in the event of a privacy breach (or suspected privacy breach). The organization should also have rules that address when and how senior management will be notified. The organization should also strongly consider contacting my Office at an early stage so that my staff can provide guidance and assistance in responding to the breach.

When faced with a breach of privacy, the first two priorities are immediate containment of the harm and, in appropriate circumstances, notification of affected parties. Containment requires the organization to identify the scope of the breach and take immediate steps to confine it. Notification involves identifying those individuals whose privacy has been breached and, in appropriate circumstances (including where required by law), notifying those individuals accordingly.

Containment should be initiated immediately. In undertaking containment, interim measures should be taken to: (i) recover the personal information disclosed in the privacy breach; and (ii) protect personal information from further theft, loss, or unauthorized use or disclosure. Where possible, all hard and electronic copies of personal information which have already been disclosed should be retrieved, and the organization should ensure that no personal information (or any copy) is retained by unauthorized individuals. At the same time, the organization should also ensure that additional privacy breaches cannot occur through the same or similar means, and determine whether the privacy breach would allow unauthorized access to any other information. Where necessary, the organization should take appropriate action to guard against further privacy breaches. This may involve changing passwords or identification numbers, and/or temporarily shutting down the system.

It is also of paramount importance that the individuals whose privacy was breached be notified as soon as possible in appropriate circumstances, including where required by law.[14] The notification should include details of the extent of the breach and the specifics of the personal information at issue. If financial information or information from government-issued documents is involved, the following should be included in the notice:

> *As a precautionary measure, we strongly suggest that you contact your bank, credit card company, and appropriate government departments to advise them of this breach. You should monitor and verify all bank accounts, credit card, and other financial transaction statements for any suspicious activity. If you suspect misuse of your personal information, you can obtain a copy of your credit report from a credit reporting bureau: Equifax at 1-800-465-7166 or www.equifax.ca and TransUnion at 1-800-663-9980 or www.tuc.ca, to verify the legitimacy of the transactions listed. If you are concerned that you may be a victim of fraud, you may request these organizations to place a fraud alert on your credit files, instructing creditors to contact*

14 See the IPC's *Breach Notification Assessment Tool* at http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=581.

you before opening any new accounts. You may also wish to review a publication of the Information and Privacy Commissioner of Ontario entitled, 'Identity Theft: How to Protect Yourself', at www.ipc.on.ca.

The notification should also advise the individual of the immediate and long-term steps that have been taken (or will be taken) to address the breach. The contact information for someone within the organization who can deliver additional information and assistance, and answer questions, should be provided.

In addition to containment and notification, it is important to learn from a privacy breach. I recommend that the organization conduct a full investigation into the breach. The primary objectives of the investigation should be: (i) to ensure that the immediate requirements of containment and notification have been addressed; (ii) to review the circumstances surrounding the breach; and (iii) to review the adequacy of existing policies and procedures in protecting personal information, in order to ensure that mistakes are corrected and future breaches avoided.

After the investigation of the privacy breach is completed, the findings of the investigation should be communicated to the appropriate individuals, both within the organization and (where appropriate) externally, to my Office and/or the persons affected by the breach.

These 7 steps have been summarized in Table 1.

Table 1

A Policy is Not Enough: It Must be Reflected in Concrete Practices

1. **Implement a privacy policy that reflects your organization's privacy needs and risks; conduct an effective Privacy Impact Assessment;**
2. **Link each requirement within the policy to a concrete, actionable item – operational processes, controls and/or procedures – translating each policy item into a specific actionable practice that must be executed;**
3. **Demonstrate how each practice item will actually be implemented;**
4. **Develop and conduct privacy education and awareness training;**
5. **Designate a central "go to" person for privacy-related queries within the organization;**
6. **Verify both employee and organizational execution of privacy policies and operational processes and procedures; and**
7. **Prepare for a possible breach – establish a data breach protocol.**

Conclusions

Privacy policies and procedures alone, without a proper strategy for implementation, will not protect an organization from privacy risks. The 7 recommendations presented in this paper provide organizations with concrete guidance on how to effectively execute an appropriate privacy policy, and have it reflected in actual practice.

Organizations should evaluate their policies and consider taking a *PbD* approach to embedding privacy into the organizational framework. *PbD*'s flexible, innovation-driven approach to achieving privacy can help to encourage organizations to both internalize the goal of privacy protection, and seek out ways to achieve it, in concrete, actionable steps. Additionally, the organization should demonstrate to senior management how each of these steps will be implemented.

Providing effective privacy training to employees on an ongoing basis will enable them to incorporate privacy protection into their day-to-day routines and minimize the risk of future privacy incidents. Moreover, having a senior privacy specialist available will enable employees to clarify and manage privacy-related concerns that may arise.

Organizations must also verify that privacy policies, procedures, and practices are being complied with. Integrating audits and informal reviews, as well as PIAs, into the organization's procedures will pre-emptively detect any new privacy challenges, and enable the organization to update its policies to deal with issues before a privacy breach develops. Finally, as a last step, should a privacy breach occur, employees should be equipped through strong protocols to take swift action to manage and remediate the situation. By embedding policies into the organizational fabric, using a *Privacy by Design* framework, the organization will be able to operate in a privacy-conscious manner, without compromising any functionality. The key, however, is to remember that a privacy policy, by itself, is not enough – it must be reflected in the practices of the organization, through a definite course of action.

**Information and Privacy Commissioner,
Ontario, Canada**

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

September 2012

Information and Privacy Commissioner,
Ontario, Canada