Building Privacy into Municipal e-Government

Mike Gurski, Senior Technology Policy Advisor
Office of the Information & Privacy Commissioner/Ontario
originally published in City Hall Online: A Progress Report on Municipal e-Government in Ontario, London, Ontario, Spring 2002

Electronic government parses into two main activities: placing government information online while ensuring its easy accessibility by constituents, and enabling online transactions. The second component is by far the most challenging and presents the most privacy challenges. Traditionally, the starting point for this second phase is high-volume businesses or services standing to derive the most benefit from increased efficiency and reduced transaction unit costs. To accomplish this, governments quickly see the need to bridge program and data silos and move to an enterprise architecture.

Because the terms privacy and security are often used interchangeably throughout the silo-bridging process, security architects usually find themselves saddled with privacy work. Privacy[1] and security are quite separate issues. At times, they can even be at odds. This article will examine the role of the privacy architect in a municipal e-Government initiative.

Security is an *organization-centric* control structure, as evidenced by access and authentication controls. Privacy, on the other hand, is a *person-centric* control structure. In other words, to be privacy protective, enterprise architecture or any component thereof, must give control to the individual – the consumer. These controls are captured in the *Fair Information Principles*[2]

Fair Information Principles

Accountability
- Organization is responsible for personal information under its control.
- Designate (an) individual(s) accountable for compliance with established privacy principles.

Identifying Purposes
- Identify purpose of information collection at or before time of collection.

Consent
- Obtain individual's consent to the collection, use and disclosure of personal information, except where exempted by law.

Limiting Collection
- Collect only information required for the identified purpose and collect this information by fair and lawful means.

Limiting Use, Disclosure, Retention
- Obtain consent of individual if information is used for other purposes.
- Retain personal information only as long as necessary for the fulfillment of those purposes.

Accuracy
- Keep information as accurate and up-to-date as necessary for identified purpose.

Safeguards
- Ensure protection of information by security safeguards appropriate to the sensitivity of the information.

Openness
- Make policies and practices relating to management of personal information readily available to individuals.

Individual Access
- Inform individual upon their request of the existence, use and disclosure of his/her personal information; allow individual to access that information, challenge its accuracy and completeness and have it amended as appropriate.

Challenging Compliance
- Allow an individual to address a challenge concerning compliance with the above principles to the accountable body in the organization.

[1] Informational Privacy: Data Protection
- Personal control over the collection, use and disclosure of any recorded information about an identifiable individual.
- The organization's responsibility for data protection and safeguarding personal information in its custody or control.

[2] Based on the Canadian Standards Association's *Model Code for the Protection of Personal Information*. Canadian Standards Association, 1995; recognized as a national standard in 1996.

(see inset on page 1). In short, they form a contract between an organization and an individual regarding how and under what circumstances that individual's personal information will be collected, managed and processed by the organization.

The best way to address privacy issues from both an efficiency and cost perspective, is to design the privacy technology or *enterprise architecture*, starting at the conceptual level and continuing through to the physical execution. Studies have shown that the usual arguments against introducing privacy into a technology solution of higher cost, lower performance and longer response times are mere fiction. A recent case study of a hospital information system in Europe that uses pseudonymous IDs, end-to-end encryption, and identity protection illustrates this point. The additional implementation cost for a privacy protective system was 1%. No performance degradation occurred.[3]

Wherever possible, encrypt – implement anonymity and pseudonymity.

One of the fundamental steps most often overlooked, is to question whether the personal information about to be collected needs to be collected. Privacy experts often refer to this as data minimization. The second step is to identify under what conditions the personal information collected can be pseudonymised or aggregated. Often the data processing that goes on through electronic service delivery does not need to use personally identifiable data.[4]

Beyond these fundamental steps a number of tools exist that can help a municipality to succeed in effectively addressing privacy issues in any e-Government initiative.

These include:

- Privacy Design Principles*
- Technology Design Principles
- Privacy Impact Assessments**
- Staffing (Privacy Architect)
- Technology Solutions
- Corporate Culture

**Can be found on the Management Board Secretariat website http://it.ojp.gov/initiatives/files/Privacy2.pdf*

***Can be found on the Management Board Secretariat website www.gov.on.ca/MBS/english/mbs*

Privacy Architect: The person responsible for ensuring that the design of a given technology or system or process provides sufficient and appropriate protection of personal information.

Courtesy P. Hope-Tindall, dataPrivacy Partners Ltd.

Examples of the first three steps are given in the *Other Related Sources* area of the *Links to Related Sites* section of the Information and Privacy Commissioner's website.[5] As well, most provinces and larger municipalities have resources for these three items. Harder to find is information regarding a necessary privacy staffing component on any IT project: the privacy architect. A privacy architect plays a key role in the

[3] Borking J and Raab C, *Laws, PETs and Other Technologies for Privacy Protection* Refereed article, 2001(1). The Journal of Information, Law and Technology (JILT).

[4] Ibid.

[5] Also available: *The Privacy Diagnostic Tool*, a downloadable file that uses a question and answer format to report on an organization's privacy effectiveness.

design and development of any municipal e-Government initiative. The privacy architect is responsible for identifying and defining the privacy requirements using existing *Municipal Freedom of Information and Protection of Privacy* legislation and any other laws that might apply. In addition, he/she must provide the analysis for the technology and data processing activities within the technology. Risk assessment, usually done by using a privacy impact assessment model, rounds out the privacy architect's tasks. Finally, he/she must make recommendations that allow for informed decisions on the part of senior executives. The recommendations need to cover not only the technological side of the equation but also the policy and educational components associated with any technology implementation.

"To survive mounting consumer anxiety … organisations need to institutionalize their commitment to protecting … customers' privacy by taking a comprehensive, whole-view approach…. The cost of a privacy PR blowout can range from tens of thousands to millions of dollars … and this doesn't include lost business and damage to the brand."

Forrester Research, Surviving the Privacy Issue, March 2001

This broader scope of responsibilities highlights an important distinction between the privacy architect and the security architect, whose focus is primarily on the system owner's concerns regarding access control through the use of encryption, biometrics and reporting mechanisms. The privacy architect, by contrast, acts in the user's interest, focusing on data collection, use, disclosure and retention. To get to those recommendations, the privacy architect needs to follow the data, starting with the question: "*Why does this need to be collected?*"

The privacy architect also needs to tackle the corporate culture of his or her organization. Often the most challenging work centers on developing a culture of privacy excellence in an organization. Education and training form the foundation stones for implementing privacy protection in the information technology and meeting the privacy expectations of a municipality's constituents. The privacy architect needs to ensure not only that the information technology and enterprise architecture is privacy-protective by design, but that the organization develops the capacity for ongoing privacy management. This involves identifying gaps in the technology design, monitoring the technology implementation, conducting privacy audits and post-implementation evaluation.

As well, the privacy architect needs to develop plans to address potential privacy gaffes.

All to often, an organization sustains long-term damage by not handling what began as minor privacy breach. Plans need to be put in place to isolate and rectify the privacy breach, notify affected parties up front and establish methods of systems analysis that identify other similar potential problems.

And, e-Government must earn the trust of a municipality's citizens in order for them to conduct transactions online. Trust grows from respect. In large part, a municipality's success in the e-Government arena will depend on its success in respecting the personal information provided during online transactions.