



# Open Advice for Ontario's New Chief Information & Privacy Officer

Moving to a High Performance Organization

Mike Gurski  
Privacy Strategist  
Head: Privacy Centre of Excellence (PCE)  
Bell Security Solutions Inc

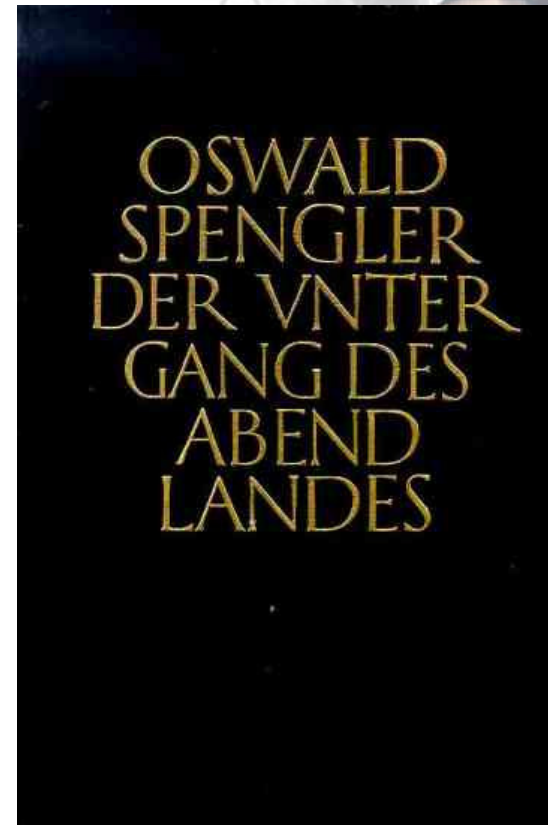
Alec Campbell  
President  
Excela Associates  
Distinguished Associate: PCE

Privacy & Security solutions



In our humble opinion...

- These suggestions are based on our experience in a wide range of public sector organizations
- The Ontario public service has achieved some notable successes in privacy administration...
- ... but there's always room for improvement
- Just ask Oswald...





## Privacy Issue Still Evolving

- Privacy remains the single most significant public policy issue in the information management space. Why?
  - With the spread of breach notification legislation in the USA, the issue's continued predominance is pretty much assured
  - The European Commission (EC) is proposing changes to European law that would require "electronic communications networks or services" to notify customers of security risks. Specifically, the changes would require subscribers to be informed of the nature of the risk, appropriate measures to take to safeguard against risk, and the likely costs subscribers will endure. Sept 13, 2006.
  - Federal Privacy legislation review for 07-08



# Why Should I Be Listening Now?

- Timing is Everything:
  - New CIPO portfolio provides a rare opportunity for Ontario Government to become a High Performance Organization with regards to developing and implementing an IM and Privacy Strategy.
- Ontario Government could benefit from an enterprise privacy strategy:
  - Engendering leadership in staff and executives
  - Shift to designing privacy functionalities into IM solutions
  - The RFP Lever
- The Value Proposition of Privacy:
  - Compliance
  - Risk
  - Cost
- More Detailed Advice



## What is a High Performance Public Service Organization?

- **1** - The right people are the origin and end of the high-performing organization.
  - Aligned, teamed, energized, capable, and pioneering people create high-performing organizations, and, reciprocally, these organizations attract, nurture, and develop these people. The relationship is circular and self-sustaining. A high-performing organization *never* acts in a way that compromises this relationship.
- **2** - People at high-performing organizations are guided by a single imperative:
  - *to maximize public service through learning.*
  - They focus on leveraging learning into perfecting the achievement of the **Ministry's intent.**
- **3** - **All elements other than people are optional.**
  - The traditional trappings of government (structure, strategy, systems, procedures, equipment, tools, and facilities) contribute nothing to its success except as they serve and are used by its people. A high-performing organization always values these trappings based on whether they empower people and enable them to achieve the full measure of their abilities.



## How Do You Become a High Performance Privacy Organization?

- Educate leadership and staff on privacy
  - Require privacy expertise in management and staff
- Uncover and remove the obstacles to high-performance and **realize the opportunities for advancement/leadership**
- Engage your people in service improvement activities that align to **Ministry Intent**, team them in making change, stimulate their energy with opportunities to make a difference, enable them with knowledge and skills, and encourage them to see privacy in new ways
- Elevate your people's ability to generate new ideas, acquire privacy knowledge rapidly, and transfer it efficiently across the government
- Conduct renewal sessions that reflect on your progress, extract learning, and fold that learning into increased privacy successes.



## A Quick Straw Poll

- Who thinks the OPS is a High Performing Service Organization Already, and why?
- Who can see the opportunities in the OPS to becoming a High Performing Service Organization? What are they?



## Why Do We Need an Enterprise Privacy Strategy?

- A Lesson From Peru:
  - The Shining Path Terrorist Organisation
    - The Dentist, the Ballerina, and Abimael Guzman
    - The tragedy of an aversion to high performing organizations.
- A Lesson from the Federal Government:
  - Is the Social Insurance Number a file tag or an identifier?
  - Is there a federal Identity Management Strategy or Policy?
- A Lesson from Quebec:
  - Minister Gauthier, IDM, My Citoyen, Cliqsecur, Privacy
- A Local Lesson
  - You know better than us.



## What are the Components of an Enterprise Privacy Strategy?

- Walk before your fly:
  - Embedding Privacy Principles
  - Privacy Acculturation
  - Strategy Articulation (applying risk management techniques)
  - Planning and Implementation
  - Missionary Work
- Achieving Cruising Altitude:
  - Ongoing education and training
  - Periodic reinforcement of importance of privacy
  - Operational reviews and Audits
  - Strategy and Plan review



## What are the Actions We Need to Focus On?

- The activities which need to be undertaken by a government agency that recognises privacy and dataveillance as being of strategic importance. It is based on the principles of:
  - a proactive stance;
  - an express strategy;
  - an articulated plan;
  - resourcing; and
  - monitoring of performance against the plan.

Public sector agencies are increasingly recognising the need to examine their operations from the perspective of their clients' privacy interests.

- Roger Clarke, May 1996

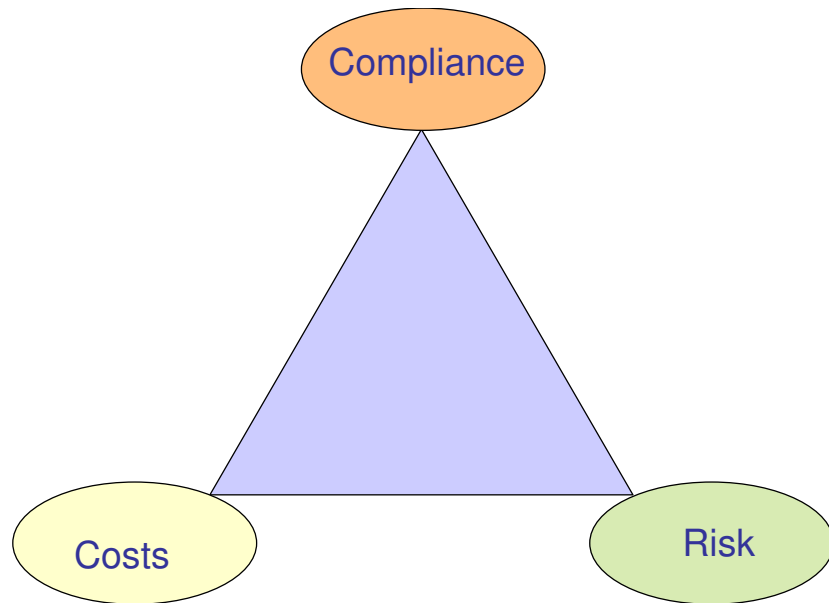


## But How Do We Know If We are There Yet?

- Take the Anonymity/Pseudonymity Test:
  - Is there such a thing as Accountable Anonymity?
  - Can you identify service transactions where the data does not need to be readily related to a particular individual?
  - What is a pseudonym?
    - **A pseudonym is an identifier for a party to a transaction, which is not, in the normal course of events, sufficient to associate the transaction with a particular human being.** Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it. **The data may, however, be indirectly associated with the person, if particular procedures are followed.**



# The Privacy (and IM) Value Proposition



- What this teaches us.
  - Integrating Risk Assessment into PIA's is critical.
  - Understanding the costs for compliance and non-compliance needs to be articulated
  - Compliance is both to legislation and citizen values and expectations



# Risk management

- Privacy planning is more effective if approached from a risk management perspective than a legal compliance perspective
  - Risk management permits the efficient allocation of resources
  - Legal compliance requires the allocation of resources to all compliance issues regardless of risk
- The PIA is the primary risk assessment tool but is an orphan and needs to expand to incorporated threat assessments – encourage it
  - Ensure that PIAs don't become bureaucratic exercises in which the completion of the PIA is more important than its conclusions
  - Ensure there PIA drives back into the IM project management cycle.
  - External expertise should be brought in to do PIAs only if the project is unusual or complex enough that internal expertise is inadequate.
  - Internal expertise should be adequate for most PIAs in a High Performing Organization.



# Privacy Strategy Contents

- Your Strategy should set out the direction for your Enterprise Privacy Architecture
- Consider enshrining privacy architecture principles in policy
  - First you need an enterprise privacy architecture
- Every jurisdiction should have a PIA policy as part of its Strategy
- Policy should be specific enough to ensure that its objectives are achieved and measurable, but broad enough to permit flexibility in its application
  - Needlessly prescriptive privacy policy creates resistance
- Recognize that Policy is not enough.



# Technology

- Privacy must be an integral design factor in all information technology systems and decisions; not after the fact mitigation
- In so far as technology is concerned, privacy and security must be considered in the same breath; it is not a balancing act, this is not the Cirque de Soleil
- Like security, privacy must be automated to be effective in high-volume, transaction oriented information systems!
- Privacy automation remains in its infancy, but sufficient progress is being made to justify its inclusion in strategic planning
- The use of expert systems, especially for privacy impact assessment, should be explored.
- Develop a privacy architecture to guide information systems development and redevelopment



## Organization

- Make accountability for privacy compliance explicit in every ministry
- Use Deputy Minister Performance Contracts
- Operational Accountability should rest with a position senior enough to speak for the Ministry but junior enough to acquire and maintain the necessary expertise. The director level is often appropriate.
- Accountability should for privacy compliance should also include accountability for privacy impact assessment.
- The role of the CIPO should be clear in both policy and practice.
  - The CIPO should have authority for government-wide privacy strategy and policy but ministries should be responsible for applying that policy. Therefore ministries must be involved in the formulation.



## Incident response

- Every ministry should have a privacy incident response plan including
  - First response accountability
  - Decision tree
  - Escalation process
- The response plan should include provisions for privacy breach notification to affected subjects



## Commissioner relations

- Establish a strong working relationship with the Commissioner and assistant commissioners: not a CRM model
- Pursue win-win strategies when on opposite sides of an issue
- Be proactive in dealings with the Commissioner; engage the IPC in Privacy strategic planning and policy development
- Increase government expectations of the Commissioner's Office
  - Strongly support an increase in IT and IM expertise and analysis at the IPC
  - Engage the IPC in significant IM initiatives from the outset and through the life of projects
  - Fully understand the mandate and responsibilities of the IPC
- Look to Alberta for an effective model for government-Commissioner relations



## Summary of Recommendations

- Develop a comprehensive Privacy Strategy
- Use threat analysis and risk management as the basis for privacy impact assessments
- Develop a privacy architecture for information technology applications
- Ensure that the role of the CIPO is unambiguous and clearly understood
- Ensure that the role of ministries in privacy compliance is unambiguous and clearly understood
- Involve the IPC to the fullest extent of its mandate
- Realise that PIA's are just one piece on the board.



## Pithy Conclusions for the CIPO:

- Focus on the people in your organisation first and foremost
- Use the strategies and policies to support their performance
- Create a privacy learning environment, reward privacy expertise
- Pilot the new high performing privacy organization
- Demonstrate privacy by design



## Contact Information

Mike Gurski  
Privacy Strategist  
Head: Privacy Centre of Excellence  
(PCE)  
Bell Security Solutions Inc  
905-751-4310  
[mike.gurski@bell.ca](mailto:mike.gurski@bell.ca)

Alec Campbell  
President  
Excela Associates  
Distinguished Associate: PCE  
780-945-0123  
[alec@excela.info](mailto:alec@excela.info)