

The USA Patriot Act – Government Briefing



Kirsten Tisdale, Chris Norman, Sharon Plater & Alexandra (Gina) Henley
September 30, 2004



Agenda



- Background
- Overview of Government Responses and Approach
- Mitigation Strategies
 - Contractual (Review of proposed amendments)
 - Legislative (Review of privacy protection measures)
- Questions

Background on the *USA Patriot Act*



- *USA Patriot Act* is a response to concerns about international crime and terrorism, heightened as a result of the events of September 2001.
- Amends powers already available to the FBI to obtain information about foreign intelligence for surveillance, interception and obstruction of terrorist activities.
 - FBI must obtain orders from a special court: the Foreign Intelligence Surveillance Court.
- Privacy concerns stem primarily from Section 215 which allow the FBI to conduct electronic surveillance, enter a facility covertly or access business records.
 - The person who is the target of the order need not be a person suspected of criminal activity or of being a foreign agent.
 - A person served with a *USA Patriot Act* order is not permitted to disclose the fact of the order to anyone other than those persons necessary to produce the items sought.

A New Global Reality



- The Patriot Act is not just an issue for governments in Canada, it is also an issue for the private sector.
- B.C.'s businesses, government and citizens live in an electronic age and are part of a global economy where personal electronic transactions occur daily.
- The potential for disclosure of personal information under the USA Patriot Act applies to personal information held by all Canadian corporations or organizations that have U.S. affiliations (e.g. VISA, Walmart, Future Shop, Yahoo, frequent flyer and bonus programs)
- The implications of the Patriot Act in the United States are much more significant than they are in Canada.

The Privacy Issues raised by the Patriot Act are about striking a balance between the need for security, the importance of privacy, and the economic realities of a global economy.

Submission to the Privacy Commissioner

The Province sought and obtained U.S. and Canadian advice to deal with concerns about the Patriot Act.

1. The risk that personal information held in B.C. could be obtained by U.S. authorities under the Patriot Act as a result of Government outsourcing initiatives is small.
2. To further reduce any possible risk to British Columbians, Government will implement enhanced privacy protection measures to ensure that a U.S. affiliate does not have access to, or control of, sensitive personal information held by a Canadian or B.C. service provider.
3. In addition, Government will propose legislative amendments that build on what is already the strongest privacy legislation in Canada by prohibiting all government service providers from disclosing personal information outside of Canada, as well as requiring that companies provide notice in the event that their foreign affiliates requests the disclosure of personal information.

Conclusion:

The Patriot Act poses a small incremental risk. However, British Columbia is a leader in privacy protection and will take effective measures to reduce that minimal risk.

Government Supports Review by Commissioner



- Government takes the protection of British Columbians' personal information very seriously and the work we have done on the USA Patriot Act is precedent setting.
- We support the public review process and have made a submission in response to Commissioner Loukidelis's request for input into the implications of the USA Patriot Act.
- We also released vendors currently working with Government from confidentiality agreements in place that would have prohibited them from making a submission to Commissioner Loukidelis.
- The submission is posted on the Government of British Columbia internet site at <http://www.gov.bc.ca/lcs/down/submission.pdf>

The *FOIPP Act* – B.C. Protects Privacy



- The FOIPP Act authorizes government to use contractors to provide services involving even sensitive personal information as long as reasonable security arrangements are in place to protect that information.
- The FOIPP Act authorizes a public body to disclose personal information to a contractor that is necessary for a contractor to provide the contracted services.
- At the same time the Act requires public bodies to implement appropriate privacy protection measures with respect to personal information in its custody or control.
- Section 30 of the FOIPP Act provides that the head of a public body must protect personal information in its custody or under its control by making **reasonable** security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Proposed Changes to FOIPP Act



- BC has the strongest privacy protection in Canada. We propose to further strengthen the legislation by:
 - Amending protection of privacy provisions in the FOIPP Act to prevent the disclosure of personal information outside of Canada by a Service Provider
 - Requiring the reporting of any requests for personal information received from jurisdictions external to Canada
 - Creating offences and penalties for violation of disclosure rules and failure to report
 - Including “whistle-blower protection” in legislation to protect individuals who report violations of the disclosure rules
- Amendments are prepared for the fall 2004 Legislative session.

Privacy Protection Measures



- The proposed amendments to privacy legislation are the first step in a two-pronged approach.
- To mitigate any small incremental risk of disclosure of Canadian personal information under the Patriot Act, the Government has also developed a rigorous set of privacy protection measures.
- There are four key objectives of the privacy protection measures:
 - Measures to limit the application of the Patriot Act – so that it doesn't apply
 - Restrict the ability of the U.S. company to compel disclosure
 - Advance notice of potential disclosure
 - Incentives and consequences to prevent disclosure

To further reduce any possible risk of disclosure of British Columbians' personal information under the Patriot Act, Government will implement enhanced privacy protection measures in its arrangements with service providers.

Privacy Protection Toolkit



- The Province has developed a set of privacy protection measures that will be deployed on a case by case basis to meet these four objectives.
- Many of these tools are not new to Government, and are already in place.
- Mechanisms that can be drawn upon to protect personal information include:
 1. Technology and Businesses Processes
 2. Employee Strategies
 3. Corporate Structures
 4. Contractual Measures
- Projects will draw on the tools according to their specific requirements. Government is not trying to impose a “one-size-fits-all” solution.

We are putting forward a broad toolkit of strategies. It's a made-in-BC solution that provides a model for the rest of Canada to follow.

1. Sample Measures: Technology and Business Processes



- Ensure the Province's security requirements (as defined by FOIPP Act, Office of the CIO, etc.) are met by the service provider
 - Include detailed privacy and security standards in each contract
 - Complete a detailed PIA for every project before proceeding
- Automated audit and notification procedures
 - Tracing and audit trails for data access
 - Notice sent to Province when unusual or unauthorized access takes place
- Limiting access to personal information (physical and logical)
 - Only employees who need access to perform their job function can access personal information (role-based access)
 - Restrictions based on passwords, IDs, encryption, restricted access to storage facilities etc. that are appropriate to the level of sensitivity of the information.
- Restrictions on data mobility
 - Data cannot leave the premises in physical or electronic formats.
 - Examples include restricting laptops, wireless technology, PDAs, ensuring that databases are not connected to networks except as necessary and proper asset disposal.

2. Sample Measures: Employee Strategies



- Projects structured so that no individual employed by the U.S. company has access to personal information unless appropriate strategies are in place to prevent its disclosure.
- Agreements directly with the Province
 - Each employee would directly contract with the Province with respect to the release, disclosure, or provision of access to personal information (including early warning systems and whistle blower provisions).
- Employment arrangements
 - Clear and enforceable contractual obligations relating to handling data
 - Hotline established for employees to call with any suspected disclosure concerns
 - Service provider agrees that complying with Province non-disclosure agreement will not adversely affect employee
- Education and training
- Special security clearance requirements for certain employees.

3. Sample Measures: Corporate Structures



- Contract only with non-US based subsidiaries
 - Require that all personal records be in the sole custody of an entity incorporated in B.C. (or pursuant to federal legislation)
 - This severs the link between the personal information and the jurisdiction of the *USA Patriot Act*
 - Require that all directors of the Canadian service provider be Canadian citizens and B.C. residents
- Ensure disclosure of personal information pursuant to Patriot Act to be outside the service provider's corporate authority
- Trust arrangement (extreme measure in limited circumstances)
 - Legal ownership of entity shares vested in Province or third party Canadian trustee
 - Beneficial owner has no authority to compel the Canadian entity to disclose personal information

The corporate relationship can be tailored to sever or limit access to personal information.

4. Sample Measures

Contractual Measures



- Expressly prohibit access to personal information by US affiliate
- Require the Canadian service provider to provide notice of a request by its US affiliate for government information
- Require that personal information be kept in Canada
- Liquidated damages
 - Provisions for payment of liquidated damages in the event of any disclosure of personal information
- Bonding/performance guaranty
 - Require service provider to obtain a performance bond that is triggered by disclosure of any personal information to its U.S. affiliate
- Termination rights
 - The Province be permitted to terminate all or part of the agreement with the Service Provider in the event of any disclosure of personal information
- Provide Province with contractual rights to take over operations in event of potential disclosure of personal information

Contractual obligations between Government and the Service Provider will strengthen the Province's ability to protect personal information.

Leading Canada in Privacy Protection

The Government's submission to the Information and Privacy Commissioner is available online at:

<http://www.gov.bc.ca/lcs/down/submission.pdf>

For more information please contact Kirsten Tisdale, Senior Advisor, Corporate Initiatives at kirsten.tisdale@gems2.gov.bc.ca

Please note: The official position of the Province of British Columbia is set out in the submission. In the event of a conflict between those submissions and these slides, the submission takes precedence.



**BRITISH
COLUMBIA**