Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/027
Agenda Item: 26

An Overview of Information Privacy

Purpose: Information
Submitted by: Canada

APEC Symposium on Information Privacy Protection in E-Government and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006

An Overview of Information Privacy

David Loukidelis
Information & Privacy Commissioner for British Columbia (Canada)

APEC Symposium on Information Privacy in E-Government & E-Commerce
Ha Noi, Vietnam
February 22, 2006

Introduction—Today's Objectives

- First, discuss what information privacy is and why it is important
- Second, discuss the role of the APEC framework in implementing information privacy principles
- Third, discuss some examples of how information privacy is protected in various economies
- Fourth, discuss some approaches for regulators to take in promoting and enforcing information privacy compliance
- Discussion will focus largely on private sector privacy issues, not public sector

1a. What is information privacy?

- Privacy has different meanings in different cultures and in different situations
- It can mean being free from unwarranted intrusion by the state into your home or your body
- Information privacy is about information, not your body or home
- It is about having some control over collection, use and disclosure of information about you as an individual
- Many see privacy as a human right (example: 1948 UN International Declaration of Human Rights)
- Others see privacy as an economic matter
- Many see privacy as a matter of individual autonomy but it is also a community interest

1b. Why does information privacy matter?

- In many cultures, people care about their privacy and are concerned about misuse of their personal information
- People may be worried about information security risks, such as ID theft, more than anything else
- But in many cultures, the concerns go further and extend to uncontrolled collection, use and disclosure of personal information by the private sector or the public sector, or both
- Information privacy matters because it offers protection against inappropriate collection, use or disclosure of our information by governments and by private sector organizations

1b. Why does information privacy matter? (cont'd)

- For example, without reasonable protections, the wrong information may be used to make a decision affecting someone, often without the individual knowing about it
- Another example is ID theft—privacy protections can help reduce ID theft risks by ensuring appropriate security for information such as credit card numbers

2. APEC Privacy Framework's role internationally

- Harmonization of privacy standards is important to ensure that privacy protections are as similar as possible across borders
- This is because different rules can inappropriately hinder or even stop trans-border data flows that are necessary for economic activity and development
- International privacy statements such as the APEC Privacy Framework are vital in harmonizing domestic laws or practices for privacy protection
- The APEC framework serves as a guide for member economies to what standards they should have, while giving them flexibility in deciding which approaches work best for their economies

2. APEC framework's role (cont'd)

- International community has for 30 years recognized the need to harmonize privacy protection in order to protect privacy and also economic activity
- Examples of international efforts include the Council of Europe Convention 108 (1978), OECD Guidelines (1980), EU Directive (1995)
- International privacy commissioners issued Montreux Declaration (2005) recognizing that work remains to be done in harmonizing privacy
- APEC framework can play an important role, perhaps working with OECD, noting growth of APEC economies

3. Approaches to information privacy

- Economies have taken different approaches to privacy protection
- Some have no protection, public or private sector
- This may be for cultural reasons or political, or both
- There may be no economic push for it
- Hong Kong China has an ordinance, or law, that specifies rules but allows the regulator to issue codes
- In Canada, public sector privacy law followed US developments in the 1970s, spreading across Canada in the 1980s to now
- For the private sector, Quebec passed a law in 1994, but rest of Canada did not act until EU Directive forced action (federal law in 2001, provincial laws in 2004)

3. Approaches to information privacy (cont'd)

- Canada also offers example of private sector action
- The Canadian Standards Association Code adopted by the business community in 1995 was a voluntary code of privacy conduct (forms the core of our federal law)
- An example of self-regulatory approaches by the private sector
- In Australia, the federal *Privacy Act* allows business sectors to adopt sector-specific codes that are largely self-enforcing
- In the US, the Safe Harbor accord with the EU allows US companies to agree to comply by Safe Harbor requirements, with enforcement ultimately being left to the Federal Trade Commission

3. Approaches to information privacy (cont'd)

- Under frameworks like APEC's, businesses are trying to find new ways to meet customer expectations, and laws, for their global operations
- Global corporations are adopting rules or codes to cover their global operations, with the codes designed to meet all legal requirements around the world
- To deal with concerns about transborder data flows, businesses are using contracts to regulate privacy issues related to transfer of personal information between companies and across borders
- EU appears to be starting to see the benefits of these approaches, which we can call 'mixed' or 'hybrid'

3. Approaches to information privacy (cont'd)

- In the transborder context, we will see more use of mixed forms of privacy protection in the coming years
- We will see private sector self-regulation and private dispute resolution in relation to transborder data flows, often within the framework of national or sub-national privacy laws and oversight of data protection authorities

4. Tools for privacy compliance

- Hybrid tools are evolving even in economies that have a traditional model that uses a privacy law and an enforcement agency
- Will now discuss examples of this from Canada, specifically, the Province of British Columbia ("BC")
- The situation is similar under our federal privacy law and in other Canadian provinces such as Alberta and Quebec
- We have a private sector privacy law in BC, the *Personal Information Protection Act*
- It is enforced by the Office of the Information and Privacy Commissioner ("OIPC"), an administrative tribunal and investigative agency independent of the government

- OIPC can receive and investigate complaints about privacy breaches or investigate without complaint
- OIPC can require a complainant to first try to settle the matter with the business involved
- OIPC can mediate settlement of complaints
- Where a complaint is not settled in mediation, OIPC can hold a formal hearing
- The Commissioner has the power to make findings on the evidence and legal determinations
- The Commissioner can make a binding order
- Fines or damages may be awarded in court
- OIPC can order an organization to cease illegal practices or destroy information

- These are very formal powers, but BC's regulatory approach actually offers a mixture of formal powers and processes and less formal tools
- OIPC also has less formal powers to promote and ensure compliance
- For example, the OIPC can comment on the privacy implications of proposed programs, policies or business activities
- OIPC can comment on the implications of data linkage proposals or automated information systems

- OIPC has an explicit mandate for public education
- OIPC can commission research into any matter affecting achieving the law's purposes
- The mixture of formal and less formal tools offers flexibility, giving the OIPC discretion as to which tools to use in specific cases and discretion in creating an overall mix of approaches

Risks & Benefits of Various Powers and OIPC Practices

- OIPC practice has, in several ways, built on the OIPC's explicit statutory powers
- Each has benefits but also presents risks

1. Providing Advice on Proposed Programs

- The OIPC is regularly asked to advise public bodies and organizations on their proposed laws or programs
- OIPC's advice often is informal, but may be written

Benefits of Giving Advice

- OIPC's advice gives organizations the heads-up, often early in the design phase, and before major commitment of funds, of privacy risks or roadblocks
- Advice-giving is pro-active and often more systemic in nature than a complaints-handling focus

Risks of Giving Advice

- Advice-giving raises the litigation risk of claim of pre-judgement, or bias, where a complaint is later made about the matter
- Giving advice can also, of course, be reactive—and focussed *ad hoc* on narrow initiatives

- It can also be difficult for the OIPC to capitalize on advice given in terms of publicizing lessons learned—advice is given in confidence, so without public body or organizational consent to disclosure, the advice only builds capacity within the OIPC
- Technical competence of regulator's staff may be raised by IT-related proposals

2. ***Publication of Support Tools***

- The OIPC's practice is to publish support tools for compliance where the OIPC has, through OIPC research or stakeholder consultation, identified needs
- Example: Guidelines for police CCTV of public places
- Example: Guidelines for contracts to outsource data processing
- Example: Privacy impact assessment tool
- Example: Model privacy policy and consent language for doctors

Benefits of Publishing Support Tools

- Support tools/resources promote both technical compliance *and* best privacy practices
- They do so pro-actively, by anticipating trends and needs

Risks of Publishing Support Tools

- Necessarily generic nature of support resources may lead to overly-general material
- By contrast, too narrow a focus leaves gaps
- Resources to invest in creating materials, or technical expertise, may be lacking

3. Sending Would-be Complainants Back

- OIPC policy is to require would-be complainants to first try to resolve their dispute with the relevant organization or trade association

Benefits of Referral-Back

- It treats privacy compliance—certainly in the private sector—as primarily a matter of customer relations
- It forces parties to private transactions to bear the costs of compliance and reduces resource demand for OIPC and thus taxpayers

Risks of Referral-Back

- OIPC loses sight of the matter, raising risk that a dispute will settle for unrelated reasons, leaving a privacy problem untreated
- Even where complaints are settled on the privacy merits, no lessons are gained for the OIPC or a broader audience

4. Mediation

- OIPC policy under both privacy laws is to refer all complaints to mediation by an OIPC mediator
- Most complaints settle in mediation—formal hearings are almost unheard of under the public sector privacy law

Benefits of Mediation

- Interests-based mediation achieves mutually-beneficial outcome at lower cost than formal hearing
- Complainant's privacy is respected—further victimization possible in formal hearing process is avoided

Risks of Mediation

- Training of mediators can be time-consuming
- Possibility that participant unhappiness with outcomes may (among other things) reduce regulator's credibility
- In any system where complaints are mostly settled through mediation, lessons learned about the law and compliance are confined to the regulator and the parties to each dispute—and this hinders broader understanding of the law and how to comply with it

5. Formal Hearings & Binding Orders

- OIPC can issue an order, after a formal hearing, that binds the respondent

Benefits of Formal Hearings & Binding Orders

- Obviously, a binding order will, subject to a successful court appeal, ensure compliance—it gives the complainant a real, personal remedy
- Publication of the decision deters bad behaviour through embarrassment (and rewards compliance where a complaint is dismissed)

Risks of Formal Hearings & Binding Orders

- They depend on complaints and are therefore reactive, *ad hoc* and bilateral
- They can be resource-intensive, yet yield small return in terms of compliance generally

6. Audits

Benefits of Audits

- With institutional data-holdings, audits can identify systemic problems and allow repair
- Educational benefits can flow from publication of methodology, targetted data-holdings or systems and outcomes (both regulator's recommendations or requirements and compliance response)

Risks of Audits

- Formal compliance audits can be very resource-heavy—in terms of staff or consultant time and expertise

- Without careful targetting of audit resources, to maximize generalization potential of outcomes, the resources invested may be wasted—but over-ambitious audits can collapse
- Example: Would it be best to audit BC's central cancer treatment agency or a small rural hospital? Would the latter yield any generally-applicable findings? Would the former swamp the OIPC's resources and expertise?

7. ***Providing Education***

- The OIPC periodically holds, around BC, training workshops and conferences (on a cost recovery basis)
- Training workshops focus on education and skills-improvement for privacy officers in public bodies or organizations—they offer hands-on, practical exercises in privacy compliance
- OIPC conferences fulfill the broader goals of generating policy discussion *and* educating the public about their privacy rights and current issues

- OIPC and staff regularly speak to seminars and conferences about privacy compliance, again to promote compliance and educate a broader audience

Benefits of Education Efforts

- Training of organization staff builds and maintains compliance capacity and promotes good practice—and it can reduce demands on OIPC resources
- Conferences maintain dialogue, over time, on merits of the legislation and assist in identifying gaps or areas for reform as circumstances evolve

Risks of Education Efforts

- Training events do not always capture the right audience—entry-level staff often attend, not IT or other program managers
- This can reduce impact in terms of capacity building or organizational cultural change
- Conferences may similarly suffer from the wrong focus
- They may also fail to target the right audience or most important topics

Concluding Comments

- The Canadian practice has—as in BC—been to combine freedom of information (FOI) and privacy oversight duties in one agency
- Incidence of demands can, as in OIPC's case, skew the agency's focus (compare the OIPC's 1,000 FOI appeals a year to the roughly 200 (public sector) privacy complaints
- Also, regardless of which enforcement tools have been given to the agency, good privacy enforcement depends on adequate resources for the agency

- For the OIPC, fiscal restraint has meant imposed budget cuts of 35%
- Remaining OIPC staff are forced to focus on responding to complaints and FOI appeals
- The government's fiscal direction has seriously undermined our ability to pursue most of the pro-active avenues identified above—advice-giving is greatly reduced, creation and updating of support tools has been greatly reduced, *etc*.

- Resource scarcity forces the OIPC into damage-control mode—pre-occupied with responding to complaints and appeals, merely keeping the listing ship afloat
- This perversely hinders or precludes strategic planning, and thus targetting of remaining resources for outreach, support and advice
- OIPC's shift from pro-active, systemic work to reactive complaints focus may increase compliance costs for public bodies and organizations in the medium term
- Without adequate resources for the oversight agency, ultimately there is a real risk of having only an illusion of data protection

Possible Elements of APEC Framework

- An oversight agency independent of government is key to public confidence and stakeholder co-operation
- A broad range of enforcement tools is desirable
- On the formal end, formal investigative powers (including audit power) and power to issue binding orders—not just recommendations—is desirable
- On the other hand, it would be useful to have general authority to comment on privacy implications of programs and laws, to educate stakeholders and the public, to issue guidance on emerging issues

- Authority for the agency to issue or approve of sectoral codes or issue guidance notes (binding or only advisory) is missing from BC's scheme—it is well worth considering
- Agency should be structured to enhance strategic planning that is crucial to an effective mix of oversight approaches, formal and informal
- Continuous, unrelenting communication with identified stakeholders is key—agency perhaps should be required to create an external advisory body (*e.g.*, Privacy Commissioner of Canada's EAP)

- Agency must be open to constructive criticism and feedback
- More pragmatically, ensuring adequate, long-term funding for the agency is critical to success for public and private sector legislation
- Independence of the agency could perhaps be best assured if a body at arm's-length to government were to set the agency's budget

Conclusion

- This presentation was intended to give you a brief description of what information privacy is, of the international context for modern privacy standards and enforcement approaches, and to offer one example of how an economy might approach oversight of privacy compliance
- The Office of the Information and Privacy Commissioner for British Columbia is always happy to provide information, assist or collaborate with privacy compliance issues
- Thank you for your kind attention

Office of the Information & Privacy Commissioner for British Columbia

Victoria, British Columbia

Canada

Email info@oipc.bc.ca

Web www.oipc.bc.ca