

**Personal Information Protection in the Face of Crime and Terror: Information
Sharing by Private Enterprises for National Security and Law Enforcement
Purposes**

Executive Summary

A report prepared by Tamir Israel, Ali Mian, Aba Stevens, and Michelle Yau
Supervised by Andrea Slane

Centre for Innovation Law and Policy
March 2008

Funded by the Contributions Program 2007-2008
Office of the Privacy Commissioner of Canada

Executive Summary

Approach of this Report

This report considers how information is shared by private entities with national security services and law enforcement, by engaging in a two layered research agenda: 1) to describe the context of information sharing by private enterprises with public bodies in four major industries where potentially sensitive personal information is typically held; and 2) to consider the statutory or *Charter* restrictions or questions that are raised by these information sharing practices. The report examines the telecommunications industry, the retail industry, the banking industry, and the airline industry in order to make recommendations.

Summary of Recommendations

Throughout analysis of information sharing in all four industries, the importance of balancing the privacy interests and rights of individuals with the investigatory interests of law enforcement and national security agencies has been a pervasive theme. The writers also considered important practical concerns of the industries. The following recommendations are the result of these efforts.

Recurring concerns include: 1) lack of clarity regarding the interpretation of s. 7(3) of *Personal Information Protection and Electronic Documents Act*; 2) the impact of technological development on the balance of relevant interests; 3) lack of transparency regarding informal information sharing, and 4) a tendency towards collection of increasing amounts of personal information identified in some of the industries. Some persistent constitutional issues are: 1) the departure from the principal of judicial authorization in the cases of information sharing without warrants or court orders, 2) lack of certainty regarding whether there is a reasonable expectation of privacy in various contexts and 3) the constitutional sufficiency of the standard for disclosure in instances where information is obtained notwithstanding a lack of reasonable probable grounds to believe that a crime has been committed. This last concern is particularly pressing where disclosure of information to national security agencies had been made mandatory.

The Executive Summary follows the structure of the report. It begins the telecommunications industry, which tended to reveal recommendations pertaining to generally applicable law, proceeds to discuss the retail sector and banking industries, and concludes with an analysis of the airline industry, with recommendations that are highly industry-specific.

➤ **The Telecommunications Industry**

The analysis shows that gaps and lack of clarity in the law have somewhat frustrated the attainment of a clear, satisfactory balance between the privacy interests of individuals, on the one hand, and the investigative interests of law enforcement and national security on the other. The problems posed by s. 7(3)(c.1) of *PIPEDA* and the discretion it seemingly gives telecommunications companies with respect to the disclosure of the personal

information of its customers were principle among the gaps in privacy protection and the privacy related controversies arising in the telecommunications industry. Making the disclosure mandatory rather than discretionary under the provision, however, would be an ineffective means of solving the problem considering the uncertainty concerning the reasonable expectation of privacy in Internet traffic data and the unclear *Charter* implications of such an amendment. Mandatory disclosure would, furthermore, be problematic due to the fact that it is a broadly applicable provision that does not circumscribe the types of personal information that may be disclosed and the fact that it would trench on the norm of judicial authorization in search and seizure law.

Even though the industry has shown itself to be responsive to the deficiencies of the law, both the state and individuals have important interests at stake with respect to disclosure under this provision and real consideration at a policy level should be given to whether Telecommunications companies are the appropriate entities to balance these interests. The report thus forwards recommendations that to a considerable extent pertain to generally applicable law but derive from the nuances and experiences of this industry.

Recommendations

1. Clarification is needed of the discretionary authority of private entities to disclose personal information of customers under s. 7(3) of *PIPEDA*, especially section 7(3)(c.1).
2. Section 7(3)(c.1) should not be amended to make disclosure to law enforcement mandatory absent a warrant, court order or other clear authority.
3. Disclosure of personal information in the absence of a warrant should be subject to consideration of the following factors: the seriousness of the crime being investigated, whether the nature of the crime is such that the inability of the state to access the information will foreclose the investigation, and whether the information is of a sort for which the privacy interest of the individual is relatively low.

➤ **The Retail Industry**

Analysis of the Canadian retail industry shows a current state of equilibrium between security and safety on the one hand and privacy rights on the other. However, the current regulatory scheme may be insufficient to maintain the current level of protection of individual privacy, especially given the likelihood of future technological developments which will make the compilation of personal information from a variety of sources increasingly sophisticated.

Recommendations

1. Customers should be informed when the information that they disclose to their retailer may be disclosed to public investigators, perhaps through the inclusion of this practice in the retailer's privacy policy.
2. The Privacy Commissioner should provide greater guidance to retailers regarding voluntary information sharing with law enforcement and national

security agencies. Given the likelihood of increased information sharing between public investigators and retailers, there should be clarification of the extent to which collaboration is permissible and desirable and under what circumstances it should take place. It may be appropriate to place certain types of personal information such as reading preferences or hobbies out of the bounds of non-consensual, warrantless disclosure.

3. Legislation compelling retailers to contribute personal information of consumers to a database similar to the Canada Border Services Agency's PAXIS database should be avoided.

➤ **The Banking Industry**

The section about banks shows an increasing tendency by the banks to retain more personal information, and that banks have not effectively indicated to clients the extent of personal information it needs to collect for many of their services. More specifically, it reveals that: major banks receive many informal requests from police to disclose bank records; even where banks keep a record of the nature and extent of informal police requests, their legality is often not assessed by an independent and publicly accountable authority; there remains uncertainty about under what circumstances bank records can be released without judicial authorization but in conformity with *PIPEDA*; and that the constitutionality of the 'reasonable suspicion' standard used by the Financial Transactions and Reports Analysis Centre in its disclosures of bank records to police is not yet certain.

Recommendations

1. Banks should provide clear guidelines to clients on what types of personal information can and must be collected for services such as investment advice.
2. All banks should keep track of the nature and extent of informal police requests for bank records, especially the authority under which these records are being sought, as well as the circumstances in which the records are disclosed.
3. An independent and publicly accountable authority, such as the Office of the Privacy Commissioner of Canada, should be tasked with assessing the legality of informal police requests for bank records.
4. Parliament should clarify terms in *PIPEDA* such as 'lawful authority' and 'national security threat' by providing examples of when personal information such as bank records can be disclosed without judicial authorization.
5. The Government of Canada or the Privacy Commissioner should bring a reference to the Supreme Court of Canada to inquire whether the standard of 'reasonable suspicion' can ever be justified to disclose personal information, such as bank records, to police in a criminal context.

➤ **The Airlines Industry**

Analysis of the airline industry shows that the balance of individual privacy interests with national security in current law and practice create the potential for infringement of privacy rights beyond what can be justified. There are a number of areas of concern. Even if an airline earnestly wanted to protect its customers' privacy, it will be hard pressed to do so when faced with the requirements of various legislative provisions which make disclosure of information mandatory absent any proof that the collection is justified. Another threat to privacy is the vagueness of the provisions of the *Customs Act* that establishes the PAXIS database. The continuous data streaming of Advance Passenger Information and Passenger Name Record information on all passengers entering Canada facilitates the authorities in fishing for information about individuals, results in a lack of transparency about police investigations, and does not accord with the plain meaning of the words in the *Aeronautics Act*. The Passenger Protect Program (no-fly lists), though helpful for protecting the safety of airplanes, would benefit from safeguards to better protect individual privacy and to reduce the probability of false listing and false matches. Given the mandatory disclosure requirements to which the airlines industry is subject, informal sharing of customer personal information with police should be limited or avoided altogether.

Recommendations

1. Legislated mandatory collection and disclosure requirements should be amended to clarify and specify conditions that must be met before an officer can compel an airline to disclose personal information of customers.
2. The legislative provisions relating to disclosure to the PAXIS database should be clarified to specify the conditions for disclosure.
3. Continuous data streaming should not be the norm.
4. Safeguards should be put in place to ensure the accuracy and minimize imprecision of the Passenger Protect Program.
5. Airlines should adopt policies to discourage informal information sharing between airline staff and government.