

UNIFORM LAW CONFERENCE OF CANADA

CIVIL SECTION

PROTECTION OF PRIVACY AMENDMENT ACT (DATA BREACH NOTIFICATION)

INTERIM REPORT 2009

Identity Theft Working Group

Readers are cautioned that the ideas or conclusions set forth in this paper, including any proposed statutory language and any comments or recommendations, may not have not been adopted by the Uniform Law Conference of Canada. They may not necessarily reflect the views of the Conference and its Delegates. Please consult the Resolutions on this topic as adopted by the Conference at the Annual meeting.

**Ottawa Ontario
August 9 to 13, 2009**

UNIFORM LAW CONFERENCE OF CANADA

INTERIM REPORT 2009

[1] The joint meeting of the Civil and Criminal Sections in 2008 directed the Identity Theft Working Group to prepare a draft Uniform Act to impose a duty on entities that held personal information to notify people of a compromise of security of that information. The Uniform Act was to be prepared in accordance with the recommendations of the report of the Working Group to that meeting.¹

[2] The Working Group was re-formed to reflect the predominantly civil aspect of this task. Its members during 2008-09 have been:

- Arghavan Gerami, Department of Justice, Canada
- John D. Gregory, Ministry of the Attorney General (Ontario)(Chair)
- Josh Hawkes, Alberta Justice
- Wilma Hovius, Department of Justice, Canada
- Heather J. Innes, Alberta Justice
- Gail Mildren, Manitoba Justice
- Jeanne Proulx, Ministère de la Justice, Quebec

Clark Dalton of the Uniform Law Conference also participated in the work of the group.

[3] The Working Group has made considerable progress in analysing the dynamics and drafting of a breach notification statute, but has not arrived at a text that it is prepared to recommend for adoption by the Conference as a Uniform Act. The current discussion draft is attached to this report. It raises a number of issues on which the Working Group would like the direction of the meeting. In some cases the issues may involve a re-opening of recommendations from 2008 in the light of our further discussions.

[4] It is worth pointing out from the start that a breach notification statute is only a small part of the

PRIVACY BREACH NOTIFICATION

work of protecting personal information. Indeed the protection of personal information can itself be seen as a part of a broader task of protecting all kinds of information from misuse.² However, the Conference has properly concluded that breach notification is capable of supporting its own legislative regime.

[5] As noted last year, privacy legislation in Canada is very diverse in a number of aspects. All jurisdictions have laws on personal information in the hands of the public sector, but only a few have legislated on personal information in the private sector (though the federal statute has a broad application). An important subset of personal information, health information, has its own set of rules in several provinces. The enforcement of the rules varied from commissioners with investigative and order-making powers through ombudsmen who also can investigate but who are limited to persuasion and recommendation.

[6] The Working Group has tried to prepare uniform legislation on breach notification that can fit into this diverse context. Uniformity is important because information on any individual may be held and communicated across the country, and because the holders of personal information often hold such information about people in different jurisdictions. If the security of the information in the control of a holder is compromised, no one is served by subjecting the holder to a dozen inconsistent obligations in response. Ideally the holder will know what rules apply, and people whose information is held will know what to expect.

[7] The discussion draft of the Uniform Act therefore aims to apply consistent principles across the country. It is written to fit into each jurisdiction's privacy legislation. It relies on that legislation for its scope – the definition of personal information to which it applies – and its administration – the authority that oversees its application.

[8] Briefly stated, the draft Act applies where a holder of personal information has reason to believe

UNIFORM LAW CONFERENCE OF CANADA

that the information has been accessed in a manner not authorized by the privacy legislation of which these rules are a part. If that access presents a risk of significant harm to the people to whom the information relates, the holder must notify them of the breach of security. In any event, the holder must notify the oversight authority, which the draft Act calls the Commissioner. The contents of the notice are set out in some detail. The Commissioner may require the holder to notify people if that has not been done, and also to notify the police. The police may delay notification for purposes of their investigation. Regulations may prescribe the contents of the notice. Penalties are provided for non-compliance with the Act.

[9] Here are the principal points that the Working Group wants to draw to the attention of the meeting.

[10] While the draft Act, and much of the US legislation that has to some extent inspired it, speaks of the “holder” of personal information, most Canadian privacy legislation applies to entities that have custody or control of such information. Custody and control – especially control – are broader concepts than just holding information. The Working Group considered two scenarios in particular: where someone collects and holds personal information for someone else (it could be one government department doing so for another); and where someone with principal responsibility to collect or use such information contracts with someone else to store or manage the information. Can such cases be covered by the term “holder”?

[11] In response, the draft Act offers section 100, which provides that personal information is held by an entity if the entity is responsible for the use, retention or disclosure of the information. This aims to ensure that someone cannot avoid responsibility to give notice of a breach of security because handling of the information has been outsourced to someone else. Whether that someone else is also covered, or should also be covered, may be less clear. Presumably people should receive only one notification for any one breach, so the Act should not multiply the number of entities obliged to give notice. On the other hand, the entity actually holding the data may be in the best position to know that its security has been compromised. Does the Uniform Act have to spell out the obligations between

PRIVACY BREACH NOTIFICATION

entities subject to privacy duties and their data service providers in more detail than it does in the discussion draft?

[12] The obligations under the draft Act arise if personal information has been accessed or disclosed in a manner not authorized by the Act (in which the notification rules are inserted). Will this be a clear enough standard? The obligations apply as well if the holder “has reason to believe” that the information has been so accessed or disclosed. Actual knowledge is not required. The Working Group discussed whether a different rule should apply where there is knowledge of a breach or only “reason to believe” that one has occurred. It decided that the purpose of notification was to deal with risk, and risk arose even in the absence of knowledge.

[13] The 2008 instructions were that the holder should notify the Commissioner of all breaches or suspected breaches, and the Commissioner would decide if notification should be made to the affected people. The Working Group preferred to cut out the intermediary and reduce delay in clear cases, by imposing the primary obligation to notify on the data holder. Where the breach causes a risk of significant harm (the test adopted by the Conference in 2008), the holder must notify. However, in any event and for any breach, the holder must notify the Commissioner. Thus the judgment about the degree of risk is subject to review by the Commissioner, and not left solely to the holder, who may have conflicting interests.

[14] The Working Group debated whether the Commissioner should ever have to decide if notification was appropriate. This might create burdensome new work on the Commissioner, and tempt data holders to avoid their responsibility to decide to notify by referring all breaches to the Commissioner to await instructions. It was suggested that the Commissioner should concern him- or herself with larger-scale security and prevention measures, and advise data holders accordingly. On the other hand, some independent review of the notification decision was useful, and the Commissioner would have the expertise – and the information about breaches – to undertake that review.

UNIFORM LAW CONFERENCE OF CANADA

[15] The test, for the data holder and for the Commissioner, is now expressed in the draft Act as a risk of significant harm. This notion is not further defined. Should it be? Should indicative factors be listed, such as the nature of the information or the number of people affected? The 2008 meeting said that the Commissioner should consider the costs of notification. The Working Group was reluctant to include that criterion expressly, as it seemed to prefer the interests of the data holder over those of the people affected by the breach. Is this right? Is the cost to the holder, or even the potential cost of remedial measures to those receiving the notice, a factor in the significance of the harm?

[16] As noted earlier, and in 2008, not all Commissioners have powers to order data holders to do anything, and not all Commissioners want such powers. How can the Commissioner's decision about the duty to notify be given effect where the Commissioner cannot order compliance? Should the Commissioner be authorized or required to publish its views on notification? It seems difficult to require compliance with "advice" from the Commissioner; that would turn the advice into an order.

[17] The draft Act says that the data holder may not give notice of a breach if the police direct that it not be given. While the needs of investigation are important, can the police be given an unlimited right to prevent people from protecting themselves, for the convenience of their investigation? Does it depend on how the breach has been discovered in the first place (e.g. by the holder, by someone whose information has been misused, by someone else?) If the Act were silent on this, would a data holder who did not disclose a breach for a time at the request of the police be able to defend against a charge of non-compliance with the Act on that ground?

[18] The draft Act provides a penalty for non-compliance with the Act itself (to notify the Commissioner and to notify the people affected) and with the order of the Commissioner. The Working Group discussed whether and how these penalties should apply to the public sector, and in particular to the Crown? Should the Crown be prosecuted for failing to give notice of a breach? This presents technical questions: often the entity subject to a privacy obligation is a government department or ministry, i.e. not a legal person. In any event does it make sense for a penalty to be paid out of one pocket of the public purse into another? Should the Crown be accountable for its compliance with the

PRIVACY BREACH NOTIFICATION

statute in some other way than penal sanctions? Is there a way to describe the public bodies that are subject to prosecution – Crown corporations? Municipalities? - and those that are not?

[19] The 2008 meeting recommended that the Uniform Act should deal in some way with remedies for those affected by a breach, notably credit reporting remedies. The Working Group noted that some provincial laws already contain such provisions. For example, Ontario's *Consumer Reporting Act*³ allows for consumers to get reports for free and in some circumstances to require that an “alert” be placed on their file with a credit reporting agency. Some efforts are being made to harmonize provincial and territorial laws on this subject. As a result, the Working Group prefers not to deal with this topic in the breach notification statute.

[20] The draft Act does not offer civil remedies for a breach, following the recommendation of the 2008 meeting not to bar civil remedies, but not to provide for statutory damages. Should the Working Group explore more options in this line? Should it consider imposing penalties – criminal or civil – for a breach of the general obligation to keep personal information secure, an obligation that is common to many if not all Canadian privacy statutes? Consider Quebec's provisions in its public sector⁴ and private sector⁵ privacy statutes.

[21] The draft Act is silent on administrative matters generally. For example, nothing is said about investigatory powers of the Commissioner. The Working Group thought that existing privacy legislation or other applicable law provided sufficient powers to Commissioners to find out the facts of particular cases.

[22] The Working Group invites comment and direction on any of the questions raised in this Report and in the comments in the discussion draft statute. It proposes to continue its work with a view to

UNIFORM LAW CONFERENCE OF CANADA

presenting a Uniform Act for adoption in 2010. Meanwhile it would like to consult with the Commissioners across the country, to gauge the realism of its proposals and their acceptability. A number of them have expressed their views in public documents, several cited in the 2008 ULCC report, and governments have internal guidelines as well for the handling of information in their hands.⁶ How closely the Working Group or the Conference should follow expressions of political will is a different question. We note in conclusion that the Parliamentary Standing Committee on Access to Information, Privacy and Ethics recently took no position on submissions from the Privacy Commissioner and the Canadian Bar Association recommending firmer notification duties.⁷

1 The report to the 2008 meeting is online:

<http://www.ulcc.ca/en/poam2/Identity%20Theft%20Working%20Group%20Report.pdf>. The resolution of the meeting is online: <http://www.ulcc.ca/en/poam2/index.cfm?sec=2008&sub=2008f> paragraph 10.

2 The broader task was sketched out in the 2008 report. See in particular paragraphs [104] to [108].

3 R.S.O. 1990 c. C.33, ss. 12, 12.1, 12.2, and 12.3.

4 R.S.Q. c. A-2.1, s. 63.1 and 162.

1 R.S.Q. c. P-39.1, s. 10 and 91.

6 For example, the federal Treasury Board's Guidelines for Privacy Breaches (March 2007) are online: <http://www.tbs-sct.gc.ca/atip-ai/prp/in-ai/in-ai2007/breach-atteint-eng.asp>.

7 *The Privacy Act: First Steps Towards Renewal*, June 2009, online:

<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3973469&Language=E&Mode=1&Parl=40&Ses=2>. See the discussion of “quick fix # 12”.

PRIVACY BREACH NOTIFICATION

Protection of Privacy Amendment Act (Data Breach Notification)

Discussion Draft 2009

This is drafted as an amending bill that would add a Part on data breach notification to the jurisdiction's privacy protection statute or statutes. For example, in Ontario, the draft Part, with appropriate modifications, might be added to Ontario's Freedom of Information and Protection of Privacy Act, Municipal Freedom of Information and Protection of Privacy Act and Personal Health Information Protection Act, 2004.

It is assumed that Acts to which the draft Part might be added already include definitions of "personal information" or a similar term or terms (for example, "personal health information") for privacy protection purposes. It is also assumed that such Acts provide for an officer or commissioner who has significant responsibility for ensuring the privacy protection provisions of the Act are respected. The draft Part uses the terms "personal information" and "Commissioner" on the assumption that these or equivalent terms are defined in the parent Act. In the case of a jurisdiction without an equivalent to a privacy officer or commissioner, the references to "Commissioner" might be replaced by references to some other appropriate person, such as a Minister or his or her delegate or an official with related responsibilities.

It is also assumed that an Act (or part of an Act) to which the draft Part might be added specifies the holders of personal information to which the Act (or part of an Act) applies. In some cases, application will be limited to entities with a public sector character. In other cases, application will be broader. The term "entity" is used in the draft Part as a proxy for entities that are subject to the parent Act or the relevant part of the parent Act in respect of the personal information the entity holds.

The draft Part is numbered Part X and begins at section 100.

The assumptions deal with the first two recommendations of the 2008 report, at paragraphs 11 and 13, and the last recommendation, at paragraph 62.

1. The Act is amended by adding the following Part:

PART X DATA BREACH NOTIFICATION

Holder of personal information

100. For the purposes of this Part, personal information is held by an entity if the entity has responsibilities under this Act respecting use, retention or disclosure of or access to the information.

Comment: See this report at paragraphs [10] and [11] above for the purpose of this provision and questions.

Unauthorized access or breach

101. (1) This section applies if an entity knows or has reason to believe that personal information held by it has been accessed or disclosed in a manner that is not authorized under this Act.

Comment: 1. The phrase “accessed or disclosed in a manner not authorized under this Act” is intended to capture intent of the wording in recommendation 19 in the Report to the 2008 meeting: “improperly accessed or disclosed”.

2. “has reason to believe” is a low threshold, which reflects the text preceding the recommendation.

Duty to notify

(2) If the unauthorized access or disclosure poses a risk of significant harm to persons to whom the information relates, the entity shall promptly notify them of the access or disclosure.

Comment: Sections 101 and 102 reflect recommendations at paragraphs 19, 29, 38, 41 and 44 in the Report to the 2008 meeting, with the important difference that the entity has a duty, under draft subsection 101 (2), to notify persons affected without direction from the Commissioner. It remains the case that the Commissioner can require notification by the entity: see subsection 103 (3).

Duty to report to Commissioner

(3) The entity shall promptly file a report respecting any unauthorized access or disclosure with the Commissioner.

Contents of report

102. (1) The entity shall ensure that the report filed under subsection 101 (3),

(a) includes the name and contact information of the person filing the report on behalf of the entity;

(b) includes information and documents respecting the circumstances of the access to or disclosure of the personal information, including but not limited to

PRIVACY BREACH NOTIFICATION

information and documents that might assist in assessing the risk of harm to persons to whom the information relates;

(c) includes the entity's evaluation of the risk of harm associated with the access or disclosure of the personal information;

(d) describes the steps, if any, that have been taken by the entity to notify persons to whom the information relates; and

(e) states what police forces, if any, have been notified of the access or disclosure.

Additional information

(2) The entity shall, in the report required by subsection 101 (3) or in one or more further reports, inform the Commissioner about,

(a) steps, if any, the entity has taken to limit the consequences of the unauthorized access or disclosure;

(b) steps, if any, the entity has taken to prevent a recurrence of unauthorized access or disclosure;

(c) steps, if any, the entity has taken to help persons who received a notice under subsection 101 (2) protect themselves; and

(d) plans, if any, the entity has made to take steps of the kind described in clauses (a), (b) and (c).

Further reports

(3) The Commissioner may direct the entity to file additional reports that the Commissioner considers might assist the Commissioner in meeting his or her obligations under section 103 and the entity shall promptly comply with the direction.

Determination by Commissioner

103. (1) A Commissioner who receives a report from an entity under subsection 101 (3) respecting unauthorized access to or disclosure of personal information shall determine whether there is a risk of significant harm to persons to whom the information relates.

UNIFORM LAW CONFERENCE OF CANADA

Same

(2) If the Commissioner determines under subsection (1) that there is a risk of significant harm to persons to whom the information relates, the Commissioner shall determine whether the steps, if any, taken by the entity to notify persons are sufficient.

Direction to notify

(3) If the Commissioner determines under subsection (2) that the steps, if any, taken by the entity to notify persons are not sufficient, the Commissioner shall direct the entity to take the steps that the Commissioner considers sufficient to notify those persons.

Same

(4) The entity shall promptly comply with a direction under subsection (3).

Notice to police

(5) If the Commissioner considers that circumstances warrant notifying the relevant police force of the access or disclosure and the entity has not already done so, the Commissioner shall,

- (a) notify the relevant police force; or
- (b) direct the entity to notify the relevant police force.

Same

(6) The entity shall promptly comply with a direction under clause (5) (b).

Police direction not to notify

104. Despite subsection 101 (2) or a direction under subsection 103 (3), an entity shall comply with a direction from police not to notify persons of access or disclosure of personal information.

Comment: See this report at paragraph [17] above for comments and questions.

Regulations, contents of notice

105. The Lieutenant Governor in Council may make regulations governing the contents of a notice given under subsection 101 (2) or 103 (3) in respect of unauthorized access to or disclosure of personal information, including but not limited to regulations requiring that a notice describe,

- (a) the scope of the personal information involved;
- (b) the type of personal information involved;
- (c) the nature and circumstances of the unauthorized access or disclosure;

PRIVACY BREACH NOTIFICATION

(d) the steps, if any, the entity has taken to limit the consequences of the unauthorized access or disclosure;

(e) the steps, if any, the entity has taken to prevent a recurrence of unauthorized access or disclosure;

(f) the plans, if any, the entity has made to take steps of the kind described in clauses (d) and (e); and

(g) the steps, if any, that persons who receive a notice might take to protect themselves.

Offence

106. (1) An entity is guilty of an offence if the entity contravenes subsection 101 (2) or (3), section 102, subsection 103 (4) or (6), section 104 or a regulation made under section 105 and is liable on conviction to a fine of not more than \$25,000 if the entity is an individual and not more than \$500,000 if the entity is a corporation.

Same

(2) If an entity that commits an offence under subsection (1) is a corporation, an officer or director of the corporation who directed, authorized, assented to or participated in the commission of the offence is party to and guilty of the offence, whether or not the corporation has been prosecuted for the offence, and is liable on conviction to a fine of not more than \$25,000.

Comment: Section 106 reflects the recommendation of the 2008 report at paragraph 52.