UNIFORM LAW CONFERENCE OF CANADA

CIVIL LAW SECTION

UNIFORM PROTECTION OF PRIVACY ACT (DATA BREACH NOTIFICATION)

Identity Theft Working Group

REPORT 2010

Halifax,
Nova Scotia
August 2010

Uniform Protection of Privacy Act (Data Breach Notification)

Identity Theft Working Group

REPORT 2010

[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 hold personal information to notify individuals the information is about when there has been 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.

[2] The 2009 meeting adjusted the recommendations to some extent, reviewed and commented on a draft Uniform Act, and advised the Working Group to consult with privacy authorities and the private sector. Over the course of the year some or all of the Working Group spoke on the phone with most of the independent privacy review bodies in Canada – commissioners/ombudsmen or staff or both – and had written and oral communications with legal and privacy groups and representatives of businesses, including the Canadian Bankers Association, the Insurance Bureau of Canada, and others.

[3] The members of the Working Group during 2009-2010 have been:

- Arghavan Gerami, Department of Justice, Canada, replaced mid-year by Jennifer Bucknall
- John D. Gregory, Ministry of the Attorney General (Ontario)(Chair)
- Josh Hawkes, Alberta Justice
- Heather J. Innes, Alberta Justice
- Gail Mildren, Manitoba Justice
- Jeanne Proulx, Ministère de la Justice, Quebec (retired April 2010)

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

[4] The Working Group wishes to point out once again that a breach notification statute is only a small part of the 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. However, the Conference has properly concluded that breach notification is capable of supporting its own legislative regime.

[5] As noted in previous years, 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 varies from jurisdiction to jurisdiction: from commissioners with investigative and order-making powers through an ombudsman model with investigative powers and a focus on persuasion, recommendation and publicity.

[6] The Working Group has prepared uniform legislation on breach notification that is intended to fit into this diverse context. Uniformity is important because information about 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 current 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 and the holders of personal information to which it applies – and its administration – the authority that oversees compliance. The Working Group acknowledges that most if not all privacy authorities in Canada have guidelines in place for responding to a breach of data security, and that these guidelines are largely consistent across the country, thanks to active collaboration. It is thought that uniform legislation would strengthen this framework in useful ways.

[8] Briefly stated, the draft Act applies where a person with control of personal information has reason to believe that the information has been accessed in a manner not authorized by the privacy legislation of which the new uniform rules are to be a part. If that access presents a real risk of significant harm to the people to

whom the information relates, the holder must notify them of the "breach of privacy". In the case of a material breach, in any event, the holder must notify the oversight authority, which the draft Act calls the privacy authority. The contents of the notice are mainly set out in regulations. The privacy authority may require the holder to notify people if that has not been done, and also to notify the police. Regulations may prescribe the contents of the notice. Penalties are provided for non-compliance with the Act.

[9] The draft Uniform Act has been affected by developments in the past year or so. When the project began, only Ontario's health information statute had a breach notification requirement.[1] By June 2010, four provinces (including Ontario) had passed breach notification statutes and the federal government has a bill on the subject before Parliament.[2] Nova Scotia introduced a health information protection bill in 2009 but it did not pass.[3] The statutes are inconsistent in their provisions.

- Ontario's Act has no 'test'; any time personal health information about an individual is stolen, lost or accessed by unauthorized persons, the 'health information custodian' must give notice to the individual. Limits may be prescribed by regulation but no regulation has been made.
- The other statutes and the federal bill all have risk-based tests: a duty to notify arises if there is a risk of harm from the breach. Alberta's Act requires notification of the Commissioner if there has been loss of or unauthorized access to or disclosure of personal information that presents a 'real risk of significant harm' to the individuals involved. The Commissioner may require the person with control of the information to notify individuals.
- The Newfoundland and Labrador Act and the New Brunswick Act require notice to the individual that his or her personal health information has been stolen, lost, disposed of, disclosed or accessed in an unauthorized way, unless the custodian of the information reasonably believes that the theft etc will not have an adverse effect on the provision of health care or on the mental, physical, economic or social well-being of the individual. New Brunswick adds an exception where the custodian believes that the breach will not lead to the identification of the individual to whom the information relates. Newfoundland and Labrador requires notification of a material breach to the Commissioner as well, and the Commissioner may recommend notification even if the Act does not require it.
- The PIPEDA provision requires disclosure if there is a real risk of significant harm to individuals, and a report to the Commissioner of a material breach. The incident requiring notice or a report is described as a "breach of security standards."

- The Nova Scotia bill would have required disclosure of unauthorized loss of data to the affected individual unless the custodian reasonably believed that "it is unlikely that a breach of the personal health information has occurred" or that there was "no potential for harm or embarrassment to the individual" as a result of the breach.

[10] The test determined by the ULCC in 2008 and reflected in the 2009 draft uniform statute was "a risk of significant harm". This was criticized by some private sector interests as too weak a test, i.e. one that would require notification even if the risk were hypothetical or speculative.

[11] Industry Canada published a model statute and commentary in 2008 as well, in which the test was "a substantial risk of significant harm."[4] The Privacy Commissioner of Canada criticized this proposed test as too rigorous, in that it would allow too many breaches to go without notice, and too much risk would accrue to the individuals whose information was improperly accessed.[5] No doubt the phrase "a real risk" was meant to be a compromise between these two concerns.

[12] The Working Group recommends adopting the Alberta/federal language as the appropriate test for notification: a real risk of significant harm. This seems right in principle and also may turn out to be a trend, or at least widely acceptable as a matter of policy. Using this language probably maximizes the chance that the uniform statute will be adopted. The Working Group prefers this direct and positive test to the 'negative option' of the Atlantic provinces, where notification must be given unless the custodian of the information believes that there will be no adverse effect on the individuals in question. It may be that the Atlantic provinces' rule will produce more notifications than the Alberta/federal rule, since neither the threat nor the harm from it are qualified.

[13] It may be noted that Ontario's internal rules for public sector privacy breaches are controlled by guidelines.[6] These guidelines require notification of individuals if there is a breach, to say what happened, the nature of the actual or potential risk of harm, and appropriate action to protect themselves. The duty to notify is subject to exceptions, if

- law enforcement determines notice would impede a criminal investigation;
- notice is not in the individual's interest (e.g., notice could potentially endanger an individual or result in greater harm to the individual);

- notice would serve no useful purpose (e.g., if all the personal information involved in the privacy breach is: already publicly available; recovered before an unauthorized party could possibly access it; or protected by technology, such as encryption, that would mean unauthorized access to and use of the data is not reasonably possible); or
- it is not possible to provide notice (e.g., identity of individuals affected by breach is not known).

[14] Ontario's rules are said by the responsible officials to provide more certainty about whether to notify or not than a risk-based test. Some other provinces take a similar approach for their public sector privacy statutes. At this time, however, the Working Group does not recommend a different approach for public sector and private sector privacy regimes.

[15] For reasons addressed in last year's report,[7] the Working Group believes that the primary duty to notify affected individuals should lie on the person with control of the information, that is, the person responsible for its security. That rule minimizes delay and puts the responsibility on the person responsible for the situation. It also reduces the workload on the privacy authority's offices. In other words the Working Group prefers the federal regime to the Albertan one on this point.

[16] Some people have criticized the federal amendments for leaving the decision in the hands of the person with control of the personal information, given that person's incentive not to embarrass itself by disclosing the breach.[8] However, in most cases the only way anyone would find out about the breach would be from the person with control over the data. It will be rare that an individual outside the holder's organization is able to detect a breach and trace it back to its origin. The question is what the person must do about a breach when it happens, and the statutes make that as clear as they can. There is no good independent way to avoid, or to find out about, a cover-up. Disincentives can be created against a cover-up, through persuasion, administration and penalties for non-compliance. Further, the broad duty to report breaches to the privacy authority can help ensure that such matters come to light.

[17] All the 'test-based' statutes say that the belief of the custodian is to be 'reasonable'. While this might go without saying, as people in control of personal information are not likely to act on their unreasonable beliefs, it does not harm the cause of uniformity to adopt this language as well. The draft Uniform Act from 2009

applied its obligations when the holder of personal information "had reason to believe" that there had been unauthorized access to the information. Framing a test in reasonable belief is consistent with this.

[18] The Working Group believes that the separate duty to report any material breach to the privacy authority is a good idea, as did some of the private sector commentators. [9]The test for doing so should be, as it arguably is in the PIPEDA amendments, less strict than that for notifying members of the public. In practice, however, the difference in tests for the report and for notification of individuals will probably have the effect that the privacy authorities will not hear of smaller breaches that may produce notification to individuals (a notice sent to a few individuals may well not be 'material'), but will probably hear of larger scale breaches that do not produce enough risk of significant harm to justify individual communications.

[19] The 2009 Report discussed whether the legislation should spell out that the obligations of the person with control of the data applied as well to anyone who held the information through that person, such as a third-party contractor. [10] No clear direction was given at the 2009 meeting. The present draft Uniform Act does not spell this out; it is implied in the description of the person who has control over personal information. None of the Canadian breach notification statutes deal expressly with third parties, though the actual content of a 'control' test may be more generally spelled out in the broader privacy statute. Some public sector statutes impose some duties directly on third parties. The issue is raised in a comment on the Uniform Act, for enacting jurisdictions to treat appropriately in their own context.

[20] Whether the privacy authority has the power to order the person with control over the information to notify individuals, if that person has chosen not to do so, is a difficult question because of the variety of statutes across Canada now. Some privacy authorities have order-making powers, some can make recommendations and can back them up with court proceedings, and some rely on persuasion, recommendations and publicity. The Working Group recommends that the Uniform Act should square bracket an order-making power with an alternative power to recommend notification. Enacting jurisdictions will decide which variant to adopt after policy discussions and a consideration of the logic of their statutes.

[21] The 2009 ULCC meeting urged the Working Group to give some guidance to those affected by the statute about what might constitute 'significant harm'. The new draft Uniform Act reflects this desire through language taken from the Alberta and federal legislation. Bill C-29 says that significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional

opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.[11] The factors that are relevant to knowing if there is a 'real' risk of such harm are described in Bill C-29 as the sensitivity of the personal information involved in the breach, and the probability that the personal information has been, is being or will be misused.[12]. Evaluating a 'material breach' involves the sensitivity of the personal information, the number of individuals whose personal information was involved, and an assessment by the organization that the cause of the breach or a pattern of breaches indicates a systemic problem.[13] Whether 'harm' should be a component of the test to report to the privacy authority is discussed in a drafting note to s. 102 of the proposed Act.

[22] The federal bill provides that the person who must give notice of the breach of security to individuals must also give it to other organizations if they are in a position to help reduce the harm caused by the breach.[14] The Working Group heard from Transunion, a company in the credit reporting business. It tended to oppose an obligation to provide free credit reports to breach victims, but it said that getting notice of a breach at an early opportunity would help it serve the people who would be requesting this kind of information once they received the notice. Other organizations that might be covered by this additional duty of notification are government agencies responsible for issuing identification documents, insurance companies, business partners of the breached organization, banks and other financial institutions.[15] The Working Group recommends including a provision to this effect in the Uniform Act.

[23] Both the Alberta Act and the federal bill leave a great deal of detail to regulations and even guidelines of the privacy authorities. The content of the notice to be sent to individuals is one example, though the bill states the basic rule, that the notice must contain "sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of the harm that could result from it or to mitigate that harm, as well as any other prescribed information."[16] Instances where notice might be given through the media rather than to individuals is left entirely to the regulations.[17] It is not the usual practice of the ULCC to prepare regulations, possibly because most uniform statutes set out rules of law rather than schemes needing administration. The Working Group takes the view that it is acceptable in dealing with breach notification rules to leave matters of detail to regulations, because the privacy authorities across the country have a practice of close collaboration in setting standards and practices. The chances that such matters will be dealt with in a uniform manner are high. The Uniform Act sets out the basics of what is in the notice, by way of a fairly detailed regulation-making power.

[24] One notable difference between the Alberta and federal provisions is that the former provides penalties for failing to notify the Commissioner as required, while Bill C-29 contains no penalties. The commentary to the 2008 Industry Canada model statute explained that the Privacy Commissioner of Canada did not in practice have problems getting businesses to follow her recommendations. In extreme cases she had the power to go to court for an order, but this had not been necessary. No need was felt for a more stringent regime. The Working Group recommends that penalty provisions be maintained in the Uniform Act, along the lines of what was in the 2009 Draft Uniform Act.

[25] The Alberta Act provides a due diligence defence to a prosecution for non-compliance. Section 59(4) says this: "Neither an organization nor an individual is guilty of an offence under this Act if it is established to the satisfaction of the court that the organization or individual, as the case may be, acted reasonably in the circumstances that gave rise to the offence." Several private-sector lawyers who commented on the 2009 Draft Uniform Act expressed concerns at the possibility of severe penalties for technical breaches of rules that involved a good deal of interpretation of what would be in the early years quite novel obligations. It would be possible to have a traditional 'mens rea' exposure to penalties for failure to follow the form or content requirements that require little judgment, but a due diligence (or reasonable conduct) defence to charges that involve failure of judgment of materiality of a breach, the reality of a risk or the significance of harm. The draft Act makes this distinction. The meeting may wish to consider if this distinction is overly complicated..

[26] The 2009 report to the ULCC raised the question whether prosecutions and penalties made sense when the breach notification rules applied to the public sector. Should the Crown be prosecuting the Crown? Should the legislature encourage transferring funds from one pocket of the public purse to another? Would not the risk of publicity and shaming be sufficient incentive to comply with the statute? On the other hand, proposing a statute that exposed private companies to severe penalties but public bodies only to a moral sanction may be felt to be inappropriate. Further, public bodies come in many forms, from ministries of the Crown to Crown corporations and a range of agencies, boards and commissions in between. One solution may not suit all cases. The Working Group recommends making no specific provision about the status of penalties for public bodies. Enacting jurisdictions can choose to soften the provisions for some or all public bodies if they see fit.

[27] The ULCC decided in 2008 and maintained the same view in 2009 that the Uniform Act should not provide civil remedies of any kind for data breaches. This policy has been maintained in the current Draft Act. Thus it does not provide for mandatory or low-cost credit reports, though the Working Group takes no position on whether such a rule would be a good idea in someone else's bailiwick, such as that of the Consumer Measures Ministers.

[28] Likewise the Uniform Act does not provide for statutory damages for the data breach or for the failure to notify according to the Act. It simply notes that the availability of a civil remedy - for the breach or for failure to notify - is not affected by the Act. It is acknowledged that the absence of statutory damages may make it difficult for people whose personal information has been compromised without notice to recover from the person who has had control of the information. Certainly the American experience has been that such suits have failed, most often for lack of proof of damages. [18] However, the consistent inability to prove damages in such cases may be in large part due to the lack of actual damages. Arguably the legislature should not provide what the evidence does not justify. This conclusion is the stronger when one considers damages for failure to give notice, and not for the initial breach – which may or may not have resulted from a breach of the obligation to take reasonable care that personal information be secure.

[29] A less formal but possibly effective sanction for a breach, and also for a failure to give notice of a breach, is public disclosure by the privacy authority of the fact of the breach and the identity of the body with control of the information. Such a disclosure is its own incentive for the organization to go to the affected people first. It also accomplishes the same goal as notification, namely to let affected individuals know that they may be at risk. In the latter role it is less effective than a notice to each individual, but it is better than nothing. The privacy legislation in each jurisdiction may already allow the privacy authority to make such a disclosure, but the Working Group recommends that a placeholder provision be placed in the Uniform Act to ensure that something to this effect appears in any applicable legislation.

[30] Here are the main changes from the 2009 Draft Act that have not already been mentioned:

- S. 100: definition of ‘holder’ not needed. The new draft reflects the common language of Canadian privacy statutes that apply to organizations with control of personal information. “Organization” is defined, following the Alberta statute, to include individuals acting in a professional, commercial or public capacity, not in an individual capacity.

- S. 101: the tests for breach and notification will reflect the Alberta and federal models. These provisions are now in ss. 102 and 103.
- S. 102: reports to the privacy authority will follow the federal pattern and their contents need not be spelled out in legislation.
- S. 103: the privacy authority should arguably have the power to ask for more information and to require/recommend kinds of action, not necessarily notification (e.g. he or she could ask for monitoring of the situation instead or in the meantime.) This is now in s. 105.
- S. 104: we should leave the relations with the police to common sense or other law. The 2009 meeting did not favour giving the police the power to decide whether or when notification would be done.
- S. 105: regulation-making power should expand to cover other topics, inspired by federal statute. This is now in s. 109.
- S. 106: the offence provision has one amount for individuals and another for other entities. The draft Act distinguishes between offences for which taking reasonable care is a defence – where judgment is needed on how to satisfy the Act – and those with which compliance is more straightforward. Directors and officers liability is to be kept. These provisions are now in s. 107.

Conclusion

[31] Some provinces may choose to implement the Uniform Act only for the public sector, being content to let PIPEDA apply to their private sector privacy interests. The Uniform Act is drafted with that possibility in mind.

[32] The Alberta Commissioner has described the "real risk of significant harm" test as "the national standard".[19] It makes sense for the ULCC to adopt that standard, considering that it is close to the principle approved in 2008[20] and responds to criticism of the 2008 federal principle[21]. The Working Group is of the view that the draft Uniform Act is appropriate for adoption by the jurisdictions in a way that will harmonize well with the best – and only generally applicable[22] – legislation.

PROTECTION OF PRIVACY AMENDMENT ACT (DATA BREACH NOTIFICATION)

NOTE:

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. For ease of reference, the draft Part is numbered Part X and begins at section 100.

It is assumed that Acts to which the draft Part might be added already include a definition of "personal information" or a similar term or terms (for example, "personal health information") for privacy protection purposes. Therefore, the draft Part uses the term "personal information" without defining it further.

It is also assumed that Acts to which the draft Part might be added provide for a body or an official (such as a privacy commissioner or ombudsman) with significant responsibility for ensuring that the privacy protection provisions of the Act are respected. The term "privacy authority" is used in the draft Part as a proxy for the body or official on whom such responsibility is imposed in each jurisdiction. The draft Part does not define "privacy authority" on the assumption that an equivalent term is defined or otherwise described in the parent Act.

It is also assumed that an Act (or a portion of an Act) to which the draft Part might be added specifies the holders of personal information to which the Act (or portion of the Act) applies. In some cases, application will be limited to organizations with a public sector character. In other cases, application will be broader. The draft Part defines the generic term "organization" broadly, but in each jurisdiction the term and its meaning will vary, depending on the terminology and scope of the parent Act.

Finally, it is assumed that the parent Act imposes on a holder of personal information the duty to protect it.

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

PART X
DATA BREACH NOTIFICATION

Definitions

100. In this Part,

"harm" includes bodily harm, humiliation, damage to reputation, damage to a relationship, loss of an employment, business or professional opportunity, a negative effect on the credit record, damage to or loss of property, financial loss and identity theft; ("préjudice")

"organization" means a corporation, partnership, association, trade union or other entity and an individual acting in a professional, commercial or public capacity but not in a personal capacity; ("organisation")

Comment: The enacting jurisdiction will choose the term that suits its own statute.

"prescribed" means prescribed by the regulations made under this Act. ("prescrit")

Breach of privacy

101. For the purposes of this Part, a breach of privacy occurs with respect to personal information if,

(a) the information is accessed and the access is not authorized under this Act;

(b) the information is disclosed and the disclosure is not authorized under this Act; or

(c) the information is lost and the loss may result in the information being accessed or disclosed without authority under this Act.

Organization to report to privacy authority

102. (1) An organization that knows or has reason to believe that a breach of privacy has occurred with respect to personal information under its control shall report the breach of privacy to the privacy authority in accordance with this section if the breach is material.

Material breach of privacy — factors

(2) The factors that are relevant to determining whether a breach of privacy with respect to personal information under the control of an organization is material include,

(a) the sensitivity of the personal information;

(b) the number of individuals whose personal information was involved;

(c) the likelihood of harm to the individuals whose personal information was involved; and

(d) an assessment by the organization that the cause of the breach is a systemic problem.

Time of report

(3) The report required by subsection (1) must be made as soon as reasonably possible after the organization knows or has reason to believe that the breach of privacy occurred and determines that the breach is material.

Content of report

(4) The report required by subsection (1) must describe the steps taken by the organization to comply with section 103 and must contain such other information as may be prescribed.

Manner, etc., of making report

(5) The report required by subsection (1) must be made in the prescribed form and the prescribed manner.

Organization to notify individual

103. (1) An organization that knows or has reason to believe that a breach of privacy has occurred with respect to an individual's personal information under the organization's control shall notify the individual of the breach of privacy in accordance with this section if it is reasonable in the circumstances to believe that the breach of privacy creates a real risk of significant harm to the individual.

Real risk of significant harm — factors

(2) The factors that are relevant to determining whether a breach of privacy with respect to an individual's personal information creates a real risk of significant harm to the individual include,

(a) the sensitivity of the personal information; and

(b) the probability that the personal information has been, is being or will be misused.

Time of notice

(3) The notice required by subsection (1) must be given as soon as reasonably possible after the organization knows or has reason to believe that the breach of privacy occurred and determines that the breach of privacy creates a real risk of significant harm to the individual.

Content of notice

(4) The notice required by subsection (1) must contain,

(a) sufficient information to allow the individual to,

(i) understand the significance to him or her of the breach of privacy, and

(ii) take steps, if any are possible, to reduce the risk of, or mitigate, any harm to him or her that could result from the breach of privacy; and

(b) such other information as may be prescribed.

Manner, etc., of giving notice

(5) The notice required by subsection (1),

(a) must be prominently stated;

(b) must be given to the individual directly, subject to subsection (6); and

(c) must be given in the prescribed form and the prescribed manner.

Exception

(6) If circumstances in which it is not feasible for the notice to be given to the individual directly are prescribed, the notice must, in those circumstances, be given to the individual indirectly.

Comment: The regulations should be drafted to give organizations the clearest possible direction on when indirect notice of the privacy breach will be sufficient.

Organization to notify others

104. An organization that notifies an individual of a breach of privacy under section 103 shall, at the same time, also notify a government institution, a part of a government institution or another organization of the breach of privacy if,

(a) the government institution, the part of the government institution or the other organization may be able to reduce the risk of, or mitigate, any harm to the individual that could result from the breach of privacy; or

(b) a prescribed condition is satisfied.

Direction from privacy authority to organization

105. (1) If a privacy authority receives a report under section 102 about a breach of privacy with respect to personal information under the control of an organization and determines that the breach of privacy creates a real risk of significant harm to one or more individuals to whom the information relates, the privacy authority may direct the organization to *[recommend that the organization]*,

(a) take steps specified by the privacy authority relating to notifying those individuals about the breach of privacy, if the privacy authority is of the opinion that the steps taken by the organization to comply with section 103 were not sufficient;

(b) take steps specified by the privacy authority to limit the consequences of the breach of privacy; and

(c) take steps specified by the privacy authority to prevent the occurrence of further breaches of privacy with respect to personal information under the organization's control, including, without limitation, implementing or increasing security safeguards within the organization.

Comment: If a privacy authority in any jurisdiction does not have the power to issue directions, this section would provide for it to make a recommendation only. In that situation, subsection (2) would be removed or altered.

Organization to comply and report

(2) An organization to which a direction has been given by the privacy authority under subsection (1) shall take the steps specified in the direction within the times specified in the direction and shall give the privacy authority reports about the organization's compliance with the direction within the times specified in the direction.

Disclosure by privacy authority

106. If a privacy authority receives a report under section 102 about a breach of privacy with respect to personal information under the control of an organization and determines that the breach of privacy creates a real risk of significant harm to one or more individuals to whom the information relates, the privacy authority may, despite section X *[insert the section of the Act that prohibits disclosure by the privacy authority]*,

(a) disclose the breach of privacy to the individuals in the manner that the privacy authority considers appropriate, if the privacy authority has given the organization a direction under

clause 105 (1) (a) and the organization has not taken the steps specified in the direction within the times specified in the direction; and

(b) disclose the breach of privacy to the public in the manner that the privacy authority considers appropriate, if the privacy authority is of the opinion that the disclosure is in the public interest.

Comment: The power of the privacy authority to disclose that a breach has occurred an important safeguard for the interests of the individuals affected. If any provision of the parent Act puts in doubt the right of the privacy authority to make such a disclosure, then that provision should be overridden. In the absence of a prohibition, this section goes without saying and is probably unnecessary in implementing legislation.

If a privacy authority in any jurisdiction does not have the power to issue directions, the wording and operation of clause (a) will need reconsideration, though the power to disclose may still be exercised as stated.

Offences

107. (1) An organization that contravenes section 102, 103 or 104 or subsection 105 (2) is guilty of an offence.

Employees and agents

(2) In a prosecution of an organization for an offence under this section, any act or omission of an employee or agent of the organization acting in the course of employment or agency shall be deemed to be the act or omission of the organization, whether or not the employee or agent has been identified or has been prosecuted for the offence.

Individuals directing management of organization's affairs

(3) If an organization that commits an offence under this section is not an individual, each of the individuals who were directing the management of the affairs of the organization at the time the organization committed the offence is also guilty of the offence if he or she failed to take reasonable care to prevent the organization from committing the offence, whether or not the organization has been prosecuted for the offence.

Defence

(4) No individual or entity shall be convicted of an offence under this section if he, she or it establishes that he, she or it acted reasonably in the circumstances that gave rise to the offence.

Penalty

(5) Any individual who is guilty of an offence under this section is liable, on conviction, to a fine of not more than $100,000 and any entity that is guilty of an offence under this section is liable, on conviction, to a fine of not more than $500,000.

Limitation period

(6) A prosecution for an offence under this section shall not be commenced more than two years after the date on which the offence was, or is alleged to have been, committed.

Comment: The enacting jurisdiction has a choice: it can choose a specific limitation period and take steps to avoid a conflict with any other legislation providing a different limitation period; or it can choose to have the same limitation period apply to this offence as to other offences under the parent statute, in which case this provision may not be necessary.

Regulations

108. (1) The Lieutenant Governor in Council may make regulations,

(a) governing the content of the report required by subsection 102 (1);

(b) governing the content of the notice required by subsection 103 (1);

(c) prescribing anything that is referred to in this Part as prescribed or that is required or permitted by this Part to be done in accordance with, or as provided in, the regulations and for which a specific power is not otherwise provided in this Part.

Content of notice

(2) A regulation under clause (1) (b) may require that the notice describe,

(a) the scope of the personal information involved;

(b) the type of personal information involved;

(c) the nature and circumstances of the breach of privacy;

(d) the steps, if any, that the organization has taken to limit the consequences of the breach of privacy;

(e) the steps, if any, that the organization has taken to prevent the occurrence of further breaches of privacy with respect to personal information under its control;

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

(g) the steps, if any, that individuals who receive a notice might take to reduce the risk of, or mitigate, any harm to them that could result from the breach of privacy.

---

1 *Personal Health Information Protection Act, 2004*, S.O. 2004 c. 3, s. 12.

2 Alberta's *Personal Information Protection Act*, S.A. 2003, c. P-6.5, was amended in October 2009 by the *Personal Information Protection Amendment Act, 2009*. S.A. 2009 c. 50 s. 25. The breach notification provisions came into force on May 1, 2010. Newfoundland and Labrador passed its *Personal Health Information Act*, SNL 2008 c. P-7.1 s. 15, in force June 1, 2010. New Brunswick followed with its *Personal Health Information Privacy and Access Act*, S.N.B. 2009, c.P-7.05, s. 49, not yet in force. The federal bill is the *Safeguarding Canadians' Personal Information Act*, Bill C-29, first reading May 25, 2010, s. 11, creating a new s. 10.1 of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, S.C. 2000 c. 5.

3 Personal Information Protection Act, Bill 64, first reading November 4, 2009, s. 72-73: http://www.gov.ns.ca/legislature/legc//bills/61st_1st/1st_read/b064.htm.

4 Industry Canada,"A Model for Data Breach Notification Reporting and Notification under the Personal Information Protection and Electronic Documents Act", June 2008.

5 "Advance Preview of PIPEDA 2.0", Remarks for the Canadian Bar Association etc, August 15, 2008. http://www.priv.gc.ca/speech/2008/sp-d_080819_e.cfm.

6 Ontario, Office of the Chief Information and Privacy Officer, "Taking the Right Steps – A Guide to Managing Privacy and Privacy Breaches" April 18, 2007.

7 2009 Report para.13-14.

8 M. Geist, "C-29: The Anti-Privacy Privacy Bill", May 26, 2010. http://www.michaelgeist.ca/content/view/5059/125

9 Such a separate duty appeared in the 2009 Draft at section 101(3) and 102 (setting out the contents in detail.).

[10] 2009 Report, paragraph [11].
[11] Bill C-29, s. 11, new PIPEDA s. 10.2(2).
[12] Ibid, new PIPEDA s. 10.2(3).
[13] Ibid, new PIPEDA s. 10.1(2).
[14] Ibid, new PIPEDA s. 10.3(1).
[15] This list is taken from the Industry Canada study, above note 3, at section 2.3.
[16] New PIPEDA s. 10.2(4). The Alberta Act provides for notice to the Commissioner, and all of its content is left to the regulations. Alberta Act s. 34.1(2).
[17] New PIPEDA s. 10.2(6).
[18] See 2008 Report para [45].
[19] In a meeting in Toronto on June 18, 2010.
[20] "a risk of significant harm" (2008 Report para. 29)
[21] "a substantial risk of significant harm" (Industry Canada model legislation, above note 4)
[22] The other relevant Canadian laws deal with health information only. The Working Group does not believe that health information should be treated differently from other personal information.