UNIFORM LAW CONFERENCE OF CANADA

REPORT OF THE JOINT CRIMINAL/CIVIL SECTION WORKING GROUP ON IDENTITY THEFT: A DISCUSSION PAPER

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.

Charlottetown

Prince Edward Island

September, 2007

INTRODUCTION

[1] Identity theft or identity usurpation[1] causes significant financial losses and often lasting consequential harm to its ultimate victims. It has been the subject of extensive study by a wide range of groups, organizations, and governments both in Canada and abroad.

[2] The topic has also been one of significant concern to this conference. Most recently, in 2006, the following resolution was passed by the Criminal Section:

> (a) *The Federal/Provincial/Territorial working group on Identity Theft should examine what ancillary orders or declarations might be made in conjunction with a criminal prosecution to assist a victim in this process* [rehabilitating their financial and other aspects of their identity]. *(AB2006-03)*

[3] The Civil Section was also considering the issue of mandatory or "breach" notification. A joint working group was then formed and tasked with the responsibility of drafting a discussion paper regarding these issues and identifying areas for further research and examination. The working group is comprised of the following individuals:

(1)	Josh Hawkes	Appellate Counsel, Alberta Justice
(2)	John Gregory	General Counsel, Policy Division, Ontario
(3)	Jeanne Proulx	Legislative Counsel, Quebec
(4)	Wilma Hovius	Counsel, Public Law Policy, Justice Canada
(5)	Erin Winocur	Counsel, Criminal Law Policy Branch, Ontario
(6)	Joanne Klineberg	Counsel, Criminal Law Policy, Justice Canada
(7)	Joe Pendleton	Director, Special Investigations Unit, Alberta Solicitor General

The Scope of the Problem:

[4] Statistical evidence from Canada, the United States, the United Kingdom and Australia all indicate that the problem of identity theft affects a large number of victims. It has a significant impact, both financial, and otherwise, on these victims and on many of the organizations that deal with them. However, differences in reporting procedures and other methodology make exact comparisons between these jurisdictions difficult. A

summary of some of the information reflecting the scope of this problem is summarized below.

Canada

[5] Phone Busters is a national fraud call centre operated jointly by the RCMP and the OPP. It is described as the central agency that collects information regarding identity theft. Figures provided by that organization indicate that between 2002 and 2006, 54,920 individuals have reported complaints of identity theft totalling $77,610,779.[2] Due to underreporting, they estimate that this figure may represent only 5% of the actual total.[3] A 2003 Ipsos Reid survey appears to substantiate that concern. In that survey, 9% of Canadians indicated that they had fallen victim to identity theft at some point.[4] Figures from the United States confirm that underreporting both to the police and to credit agencies is a significant problem. Some studies reveal that a majority of identity theft victims did not contact police or credit reporting agencies.[5]

[6] Information conveyed by two major Canadian credit bureaus and the Canadian Council of Better Business Bureaus reveal a higher incidence of identity theft than revealed by the Phone Busters data. These groups estimate the loss caused by identity theft in 2002 at 2.5 billion dollars.[6] The fact that identity theft may be reported to a number of different organizations, each with differing definitions and data standards further complicates the task of gathering accurate statistical information.[7]

United States

[7] A national crime victimization survey in 2004 revealed that 3.6 million households, representing 3% of households in the United States, reported that at least one member of the household had been the victim of identity theft during the previous six months. The estimated economic loss associated with identity theft was approximately 3.2 billion dollars.[8] Identity theft complaints represented 37%, or 255,000 complaints filed with the Federal Trade Commission in 2005.[9] A 2006 Identity Fraud Survey Report indicates that while the number of victims declined from 10.1 million in 2003 to 8.9 million in 2006, the total amount of those losses have increased to 56.6 billion from 53.2

billion in 2003.[10] While a 2007 industry financed survey showed a decline in the total attributable to identity theft, this survey has been the subject of controversy and strong criticism.[11]

United Kingdom

[8] A 2002 Cabinet Office Study estimated the cost of identity theft at £1.3billion, per annum.[12] An updated estimate of this figure in 2006 was £1.7 billion annually.[13] However, these figures include estimated costs to various government departments and law enforcement agencies.[14] Similar costs may not have been included in the estimates of other jurisdictions described above. CIFAS, a not for profit consortium comprised of industry and other groups reported 66,000 cases of identity fraud in 2005, compared with 9,000 in 1999.[15]

Australia

[9] Aggregate figures of all types of fraud illustrate that it represents one of the most significant areas of criminal activity in Australia. It is estimated to cost approximately 5 billion dollars annually.[16] Identity theft represents a large portion of this total with an estimated annual cost of between 2 and 3.5 billion dollars. In addition, several jurisdictions have noted that the assumption of another identity can be related to other criminal activity and can give rise to national security concerns. [17]

Victim Impact

[10] Generally speaking the impact of identity theft can be divided into two broad types; direct financial harm, and indirect harm to credit ratings, financial reputations, and in some cases, the creation of erroneous criminal records in the name of the victim.[18]

[11] More recently, two successive surveys by the Identity Theft Resource Center in the United States provide detailed information regarding the personal impact of identity theft. In 2003 and 2004 victims of identity theft were provided with a questionnaire designed to identify and describe this impact. In both studies the sample size was small, 180 and 197 respectively. The Center recognized the limitations inherent in the samples for both surveys, and indicated that further research was necessary. With that caveat, the

surveys provide a useful illustration of the nature and duration of the impact caused by this crime. A broader survey was conducted for the U.S. Federal Trade Commission in 2003. It involved interviews with a random sample of over four thousand individuals. Some of the results of those three surveys may be summarized as follows:

Discovery of Identity Theft

> *When asked how they first found out that their identity was stolen, the responses varied greatly over more than the two dozen possible answers on the survey. As in 2003, about 85% of the victims found out about the crime in an adverse manner. That means that only about 15% of all identity theft victims found out about the crime due to proactive measures taken by businesses.*[19]
>
> *Where the identity theft was limited to the misuse of existing accounts, 20% of victims were notified by banks or credit card companies. However, where the theft resulted in the creation of new accounts or other frauds, only 8% of victims were notified by banks or credit card companies. 18% of these victims were notified by other parties, including debt collectors and government agencies.*[20]

Time Spent by Victims in Restoring or Repairing Financial History

> *The Identity Theft Resource Center reported that in 2004, half of the victims spent under 100 hours (median). However, half of the victims spent more than 100 hours. When averaging total hours in repairing the damage done by the thief (without outliers), the result is 330 hours (mean). The total reported hours ranged from 3 hours to 5,840 hours.*[21]
>
> *The FTC 2003 Identity Theft Survey Report noted that on average, victims reported spending 30 hours resolving problems related to identity theft. Victims who had new accounts opened as a result of the identity theft spent 60 hours resolving these issues.*[22]
>
> *In both years, [2003-4] 26 to 32% responded that they had been dealing with their case for a period of 4 to 6 months. About 17% reported spending between 13 and 23 months on the case. However, a higher number of respondents in 2003 (23%) as compared to those in 2004 (11%) responded that they had been dealing with their case for a period of seven months to a year. A higher number of respondents reported spending more than four years on their cases in 2004 compared to those who responded in 2003.*[23]

Consequences of Identity Theft

> *Other forms of identity theft were also reported by respondents in the FTC survey. Twelve percent reported that thieves had committed financial crimes that resulted in warrants being issued in the victim's name, followed by 18% who indicated that some form of drivers' license was obtained with their information.*[24] *15% of victims reported that their personal information was misused in non-financial ways. Four per cent of that group reported that their identity had been used by an individual when stopped by law enforcement authorities or charged with a crime, most commonly to present a false identification when stopped by law enforcement authorities.*[25]
>
> *64% of identity theft victims where new accounts or other frauds were committed identified problems in relation to a number of other areas including credit or banking problems, difficulties with collection agencies or civil suits, insurance or loan rejection. 14% reported that they were the subject of criminal investigation as a result of the identity theft.*[26]
>
> *The Identity Theft Resource Center also noted that identity theft victims reported a number of other negative effects including difficulty in obtaining credit, significant difficulties in clearing their credit histories, and problems obtaining insurance. Nearly two thirds of respondents expressed having difficulty in clearing their credit histories. Negative information was put back in their credit history in 27% of the cases, or in 25% not removed in the first place. A further difficulty arose when in accurate information was sold to collection agencies, or when "fraud alerts" placed on their credit files were ignored and new credit was improperly extended.*[27]

Benefits of Early Discovery

> *The cost of an incident of identity theft is significantly reduced if it is discovered quickly. When the misuse was discovered within five months, the value obtained was less than $5, 000 in 82% of the cases. When the theft was discovered six months or more after onset, the total was $5, 000 or more in 44% of the cases. Early detection also reduces the cost and time spent by victims in rehabilitating their credit histories.*[28]

THE ISSUES

Victim Assistance using the Criminal Law

The Approach in Other Jurisdictions:

[12] The working group examined two options for assisting victims under the criminal law. The first of these represents a general approach to victim assistance in the context of identity theft. The second reflects a narrower approach designed to assist victims where the identity theft has resulted in erroneous criminal records or other entries in law enforcement or government records or databases.

The Broad Approach

[13] In 2003 the state of South Australia passed legislation providing for a certificate designed to assist victims of identity theft. For ease of reference, the provision is reproduced below:

Certificate for Victims of Identity Theft

[14] A court that finds a person guilty of an offence involving

(a) the assumption of another person's identity; or

(b) the use of another person's personal identification information, may, on application by a victim of the offence, issue a certificate under subsection (2).

[15] The certificate is to give details of

(a) the offence; and

(b) the name of the victim; and

(c) any other matters considered by the court to be relevant. [29]

[16] Subsequently, the state of Queensland adopted a similar provision, and this approach was later adopted by the Model Criminal Law Officers Committee of the Standing Committee of Attorneys General. [30]

[17] The committee noted some shortcomings associated with this approach, including the fact that the certificate itself is not a remedy.[31] Rather, it simply represents a convenient form in which to summarize the relevant findings of the Court. They suggest

that such certificates should perhaps be available even in the absence of a conviction where there is sufficient proof that an individual's identity has been misused, or notwithstanding the acquittal of a defendant, if the use of the identity of the victim is established on a balance of probabilities.[32]

[18] Other groups have also noted shortcomings with this certification approach. For example, the Australian Centre for Policing Research observed that such certificates may only be issued after conviction, and that the resulting passage of time may significantly diminish the benefits of such a document. One suggested alternative was to empower investigating authorities to issue such a certificate at various stages of the investigation which could record the police view that, on a balance of probabilities, the individual was a genuine victim of identity theft. However, they noted the objections of two police agencies to this variation. Notwithstanding these shortcomings, they endorsed the victim certificate model as described in the statutes reproduced above.[33]

[19] An approach similar to the variation suggested by the Australian Centre for Policing Research was proposed in Michigan consumer protection legislation. In 2003, the State Senate enacted a Bill providing that an individual who was the victim of identity theft could apply to the County Prosecuting Attorney, or to the Attorney General for a certificate stating that he or she was the victim of identity theft. The application would be in writing, and under oath. Among other things the certificate would contain a declaration that the individual had been determined to be a victim of identity theft. The certificate would also constitute an official state record. Although passed by the Senate, the Bill was not passed by the House, or enrolled.[34]

The Narrow Approach

[20] The State of California has adopted a narrower approach to the use of certificates to assist victims of identity theft. The state has defined "criminal identity theft" as identity theft that occurs when a suspect in a criminal investigation identifies him or herself using the identity of another innocent person. This may result in the creation of police and court records which erroneously identify the victim as a person arrested, released subject to conditions, or subject to an arrest warrant or conviction.[35]

[21] A victim of criminal identity theft may apply for a declaration of factual innocence, or the prosecution or the Court may seek an expedited declaration to that effect. Depending on the circumstances, the procedure can be complex and the applicant may bear the onus of establishing that no reasonable cause exists to believe that the applicant committed the offence in question. If granted, the order compels the sealing and destruction of the records in question.[36] Further, any police reports or records that make reference to sealed arrest reports must indicate that the individual has been exonerated.[37]

[22] Once a declaration of factual innocence is granted the victim may apply for inclusion in the Identity Theft Registry. The Registry can then be accessed by the victim, or by individuals and agencies authorized by the victim, or criminal justice agencies to verify that the individual has been a victim of identity theft.[38]

[23] Several states including Colorado, Illinois, North Carolina, and Connecticut also use the "factual declaration of innocence" model. Similar provisions have also been introduced in Minnesota, Wyoming, and Arizona[39]. In Connecticut, provisions allow for a court order directing the removal of false information from public records.[40] This approach has also been recommended by the Federation of State Public Interest Research Groups, and is included in the "Model State Clean Credit and Identity Theft Protection Act".

Applicability of Either Approach in the Canadian Context

The Broad Approach

[24] Historically, the approach to victim assistance in the *Criminal Code* has a narrow focus. Sections 738-741.2 address the circumstances in which a restitution order might be made either to the victim or to others, together with provisions relating to the enforcement of such orders, and of the relationship of these provisions to other civil remedies.

[25] The constitutional division of powers between the federal criminal law power and that of the provinces in relation to property and civil rights operates as a both a constraint

on and a necessary context within which the discretion conferred by these sections must be exercised.[41] Mindful of that constraint, the Court noted that the restitution provisions were not to be used to resolve complex or contested issues regarding the value of the property or loss, or the interpretation of written documents or agreements.[42] The Court also noted that the application for compensation be directly associated with the sentence imposed "*as the public reprobation of the offence.*"[43]

[26] The reality of this constitutional constraint must be carefully considered in relation to adopting any form of the broad approach either in use or recommended for adoption in Australia. At a minimum, such a constraint may limit the impact of any certificate to a declarative one only. As noted above, limiting the certificate in this way has been criticized in Australia. A remedy of such limited use may not be worth implementing in the first place.

[27] In addition, the limits inherent in any order tied to the criminal process must be carefully considered. As noted above, an approach tied to a criminal prosecution would be delayed by the time it took to conclude those proceedings, together with any related appeal periods. Such delays may have a particularly significant impact both in relation to rehabilitating the credit history of a victim, and limiting the amount of loss. Victim surveys indicate that both of these objectives are undermined by the passage of time.

[28] Any consideration of a remedy tied to the criminal process must also give careful consideration to the very significant underreporting of identity theft noted above. If most cases of identity theft are not even reported to the authorities, a remedy which is only available upon a criminal conviction would be of use to but a small number of victims. Finally, the recommendation of any remedy associated with the criminal process must be examined in light of existing civil practices and remedies. For example, many Canadian jurisdictions advocate the use of a standardized "Identity Theft Statement" in contacting credit reporting agencies and others in the process of recovering from identity theft.[44] Great care must be taken to ensure that any additional certificate or declaration obtained in the criminal process does not become the de facto standard, displacing or diminishing the effectiveness of existing practices and procedures.

[29] Parenthetically, it should be noted that the working group did not examine any other potential uses of the power to order restitution in the *Criminal Code.* Issues

surrounding other uses of restitution in the context of identity theft are beyond the mandate of the group.

The Narrow Approach

[30] Identity theft that results in the issuance of criminal process or a criminal conviction in the name of an innocent party is a serious problem. Related to these issues is the appearance of the name of an innocent party in local or national police records or databases where a party under investigation has used the identity of an innocent person. These problems may be exacerbated by information sharing between jurisdictions or entities within Canada or internationally.

[31] While the problem is undoubtedly serious, further research is needed to determine the extent to which identity theft results in erroneous information in law enforcement and other databases in Canada. In addition, the constitutional and regulatory context governing these resources should be carefully examined. Finally, any proposed solutions would have to be assessed against current practices in order to properly evaluate the utility of a similar approach in Canada.

Mandatory Breach Notification

[32] This working group was also tasked with examining the legal and policy issues relating to mandatory reporting of data loss. This topic is generally known as “breach notification”, i.e. a requirement that custodians or holders of personal information must give notice that personal information has been lost or the security of that information compromised.

[33] One of the main objectives of a mandatory breach notification rule is to enable potential victims of identity theft to protect themselves against the risks incurred as a result of the loss of their personal information. This notification may enable individuals to take steps to protect themselves against identity theft. These steps may include monitoring their financial information more closely, actively monitoring their credit rating, contacting credit reporting agencies, or changing their credit card numbers, bank

accounts etc. The most effective measures to minimize the risk of identity theft continue to be the subject of debate.

[34] Credit card issuers, banks, or other groups may also take steps to respond when they discover that personal information relating to clients or customers may have been improperly disclosed or accessed. For example, the Canadian Imperial Bank of Commerce recently issued new Visa cards, with new numbers, when a subsidiary of the bank feared that personal information had been lost.

[35] These steps, taken either by an individual or by card issuers, banks, or others, result in costs being incurred both directly and indirectly. In addition, there are further costs incurred by the custodian or holder of the personal information in question. These can take the form of direct costs to mitigate damage and in long-term damage to the reputation of the custodian or data holder. These costs can be significant, and the potential long-term costs may force these parties to pay more attention to the security of personal information.

[36] This portion of the report identifies some of the major policy and legal issues that would need to be addressed in relation to the issue of mandatory breach notification.

[37] It should be noted at the outset that this is not a question of first impression in policy or law. Most American states, beginning with California in 2002, have laws requiring some kind of notification of some kinds of breaches of security of personal information. At the federal level, several bills have been introduced but without success.[45]

[38] In Canada, only Ontario's *Personal Health Information Protection Act* [46] has a notification provision. Some governments have policies on the topic and privacy commissioners have contributed to the discussion. Several public interest advocacy groups have promoted notification as well. [47]

[39] This part of the discussion will consider four specific issues relating to breach notification, as well as other civil remedies for breaches of data security that might help the individuals whose data are involved or others affected by the breach, and will conclude with a word on measures to protect personal data from breach:

i) What is a breach?

ii) Who determines that a breach has occurred?

iii) Who gets notice?

iv) What law reform is needed?

i) What is a breach?

[40] Identifying the threshold at which notification is required is a critical issue. Breach notification may have significant ramifications for individuals and organizations. Identifying the proper threshold for notification requires consideration of a broad spectrum of circumstances in which personal information may be lost, or the security of that information compromised.

[41] At one end of the spectrum are the cases where personal data has been deliberately targeted and copied from databases. Less clear are cases where storage media, such as tapes, external hard drives, or laptop computers containing personal information have been stolen. News headlines are replete with examples of this type of theft.

[42] These latter cases raise a number of questions regarding the actual risk of dissemination of the personal information in question. For example, was the information or the computer or storage device the actual target of the theft? Given the levels of publicity relating to data breaches, and the value of personal information, it seems unlikely that many thieves would be unaware of the potential value of this information.

[43] More difficult questions arise when the security of personal information is "compromised" without an outright theft. It may be difficult, or impossible, to determine whether personal information was accessed, or copied, in the course of an unauthorized access to the computer system or database. Other related events, such as the disabling of security or access control systems, may give rise to a concern regarding unauthorized access. Proper identification of the circumstances that trigger the obligation to notify poses both technical and legal difficulties. In addition, care must be taken to ensure that

these thresholds are described in a "technologically neutral" fashion, so as to avoid the need for continual amendment to keep pace with advances in technology.

[44] The nature of the personal information in question may also be a relevant consideration in determining the appropriate threshold for mandatory notification. Personal financial information or a Social Insurance Number that can be used to generate other forms of identification may be more sensitive than a simple name, address and phone number. Personal health information can be very sensitive and open to abuse.

[45] In relation to classifying the sensitivity of the personal information in question, it might be useful to consider the nature of the risk occasioned by the loss of the information. For example, in the loss of information may give rise to:

> Physical concerns – that the information might be used to find the home address of an individual,
>
> Transactional concerns – that the information might be used to obtain credit or conduct other transactions in the name of the individual, and,
>
> Informational – that the information might reveal some private or personal facts – such as a health condition or other personally sensitive matter.

[46] Since the purpose of notifying people of the breach is to allow them to minimize the risk of misuse of the data, many of the laws on the topic, including California's leading model, exempt organizations from notification if the information was not likely to do harm, notably because it was encrypted. Storing personal data in encrypted form gives a safe harbour from the obligation to notify. Most US statutes do not specify the kind of encryption needed. Some systems are far more secure than others.

[47] In the absence of legislation but to promote good practice, Ontario's Information and Privacy Commissioner has recently published material [48] on the standards for encrypting personal information on mobile devices (the most likely to be lost or stolen). She recommends strongly against storing any such information on such devices, but if it must be done, then only high-power encryption meets acceptable standards. The Fact Sheet is a useful primer on different methods of encryption and their vulnerabilities. One

could consider whether such standards should be mentioned in a statute on notification for breach, or at least in accompanying regulations.

(ii) Who determines that a breach has occurred?

[48] Who decides if a sufficient breach has occurred? Should a breach notification requirement be imposed on any "compromise" or potential compromise, or should the custodian of the data be allowed to decide if the incident has created sufficient risk to notify people? One does not want to cause concern and inconvenience where none is due. On the other hand, the bad publicity from notifying people of a breach will be a strong disincentive to disclose, and may distort judgment about the seriousness of the breach.

[49] Most US statutes do not give discretion to the custodian of the data if the compromise or breach meets the statutory definition. The legislation varies widely, however, and different combinations of definition and duty can have different effects.

(iii) Who gets notice?

[50] Most statutes on the subject, including Ontario's PHIPA, require that notice be given to the people whose personal information is compromised. However, some require that notice be given as well to privacy regulatory authorities. In the spring of 2007, the federal Standing Committee on Access to Information, Privacy and Ethics reported on its five-year review of the *Personal Information Protection and Electronic Documents* Act (PIPEDA).[49] The Standing Committee recommended that notice of breach under PIPEDA be given only to the Privacy Commissioner of Canada, and not directly to the people who might be affected. The Commissioner would discuss the circumstances and determine the need for notification and relevant parameters. Thus the decision would not be left entirely in the hands of the custodians of the information, who as noted may be inclined to err on the side of silence. One may ask, however, if the Commissioner should have to get involved in deciding if people need protection from a breach of security of their information. Why not let the people decide directly, once the holder of the data has notified them of what has happened? Is the filter designed to protect people from being

unduly upset,[50] or to protect the data custodians from the bad publicity resulting from the breach?

[51] Other related issues must also be considered including the form of the notice, and what other information might accompany the notice. For example, whether a notice in the newspaper would suffice, or whether some other form of personal notification might be required.

iv) What law reform is needed?

[52] This question has two elements. First, is legislation needed on breach notification, or are other alternatives sufficient? Second, is there a unique role for this Conference, in light of the ongoing efforts of many other government and non-governmental groups and organizations in this area?

a) Is legislation needed?

[53] Arguably, notification of security breaches is the accepted response. That is certainly the case in the United States. Companies that are slow to disclose a breach suffer adverse consequences both on the stock market and in customer relations. In addition, as described in greater detail below, there is a significant and growing body of recommendations and guides issued from government agencies and Privacy Commissioners.

[54] The main regulator of privacy policies at the federal level in the United States is the Federal Trade Commission (though there are sectoral authorities in fields with their own privacy legislation). The FTC recommends that businesses notify law enforcement agencies and affected individuals and businesses where the loss of information may result in harm. It also lists factors to consider in deciding whether to notify individuals. [51]

[55] California, the pioneer in breach notification, has published guidelines under the title “Recommended Practices on Notice of Security Breach Involving Personal Information.”[52]

[56] In Canada, the Standing Committee's report on PIPEDA noted that the Privacy Commissioner already discusses breaches with companies and counsels them on disclosure. The Commissioner has issued a guide in relation to this practice.[53]

[57] The Treasury Board Guidelines for Privacy Breaches apply to breaches in the government and the discharge of the government's obligations under the *Privacy Act.* The Guidelines contain a long list of information that it "strongly recommends" be disclosed to affected individuals "to the extent [that such disclosure is] possible".

[58] At the provincial level, the Information and Privacy Commissioner of Ontario and her British Columbia counterpart have published a "Breach Notification Assessment Tool".[54] It states: "[o]rganizations that collect and hold personal information are responsible for notifying affected individuals when a privacy breach occurs." No legal authority is given for this statement. The document then analyses six "risk factors" that should be evaluated in deciding whether or not to give notice. It also lists factors that should be considered in deciding how to notify individuals (directly or indirectly) and what information to include in the notice. It concludes with a list of others that might be contacted, starting with law enforcement officials and including as well the relevant privacy commissioner(s). Additional resources available from the British Columbia commissioner include "Key Steps in Responding to Privacy Breaches", and a "Privacy Breach Notification Form" for use in notifying the Commissioner of a breach.[55] The Ontario privacy Commissioner has also issued guidelines for governments that have suffered a data breach. [56]

[59] At present, there is a division of opinion as to whether a mandatory duty to notify is needed. For example, neither the federal nor British Columbia privacy commissioners recommended mandatory notification when testifying before the recent parliamentary review of the Personal Information Protection and Electronic Documents Act (PIPEDA). In particular, the British Columbia commissioner testified "we should wait for evidence that mandatory notification actually is a cost effective way to reduce risks, for example, of identity theft flowing from a so-called data breach".[57]

[60] Concern has also been expressed regarding the impact of breach notification on the liability of data holders for any loss that might result from the breach. It would be

counterproductive if the effect of notification was to provide a shield for the data holder, while passing on all of the responsibility for mitigating the losses to the ultimate victim of the breach. Further study of this issue is needed to determine the ultimate impact of breach notification schemes in this regard.

[61] However, the Ontario Commissioner advocates such legislation,[58] as do many public interest groups like the Public Interest Advocacy Centre (PIAC)[59] and the Canadian Internet Policy and Public Interest Clinic (CIPPIC).[60] A principal argument is for consistency of practice. A voluntary system, however persuasive, creates uncertainty of interpretation and application, and may, at least in the short run, reward less scrupulous or forthcoming custodians of personal information.

(b) A Role for the Uniform Law Conference?

[62] The second question in this part is whether there is a role for the Uniform Law Conference. Various aspects of the topic of identity theft are presently the subject of study by several working groups, public-interest groups, and privacy commissioners within Canada and in other countries.

[63] For example, the federal-provincial-territorial Consumer Measures Committee has published an extensive discussion paper, "Working Together to Prevent Identity Theft",[61] that covers many of the issues canvassed here. To date the Committee has made no recommendations, and Industry Canada, the Committee's sponsoring department in Ottawa, also made none to the Standing Committee's review of PIPEDA. A 2005 study undertaken by the Alberta government revealed 15 different governmental committees and working groups examining aspects of the issue, together with a further 14 industry or regulatory groups with present or planned policies on the topic. Québec's legislature has adopted several provisions in its legal framework for information technology and privacy and consumer legislation to prevent usurpation of identity. These provisions also create obligations that can lead to civil and penal remedies». Quebec also participates in a Inter-jurisdictional Identity Management and Authentication Task Force in order to develop means, including risk management methods, to prevent usurpation of identity.

[64] However, we are of the view that a compelling case can be made in favour of a consistent approach to this issue by all levels of government. Many organizations in Canada have operations in more than one province or territory and hold data from individuals in more than one jurisdiction. They would greatly benefit from uniform rules about responding to a data breach, even in the absence of uniform global legislation.

[65] In any event, the federal government may benefit from cross-Canada policy development on the topic. That would have the additional advantage of facilitating harmonized provincial, territorial and federal legislation, which could avoid difficult constitutional issues about the appropriate scope of statutory duties at each level of government.

[66] In addition, PIPEDA does not cover several important kinds of information, such as intraprovincial employment information or non-commercial uses of information, or the actions of governments as data holders or custodians. Policy development with a uniform multi jurisdictional approach would have the advantage of providing a broader scope of consistent protection across the country.

CONCLUSION

[67] Identity theft represents a significant and growing problem. It causes large financial losses and, in many cases, lasting harm to its ultimate victims. In light of these facts, it is hardly surprising that this topic is the subject of several existing working groups including a Federal/Provincial/Territorial working group, the Consumer Measures Committee working group, the recently completed Parliamentary review of PIPEDA (Personal Information Protection and Electronic Documents Act), several Privacy Commissioners, and several initiatives undertaken by various provincial governments. International efforts, such as the work of the Model Criminal Law Officers Committee in Australia, are also ongoing.

[68] The work of each of these groups will need to be monitored to ensure that there is no unnecessary duplication or overlap in any future work undertaken by this Conference. This working group was tasked with the examination of two narrow questions. As is evident from the length of this report, even such narrow issues give rise to complex

questions requiring detailed consideration. As a result, care will also need to be taken to ensure that the scope of future mandates is discrete enough to allow for appropriately detailed consideration.

[69] Three broad conclusions emerged from the experience of this working group that may assist in shaping any continuing or new mandates to be undertaken by the working group:

[70]

(1) Empirical research indicates both that identity theft is significantly underreported to police or other agencies, and that time is of the essence in providing effective assistance to victims in overcoming the effects of identity theft. As a result, this suggests that with the exception of the “factual declaration of innocence" approach described above, civil remedies may provide more timely and effective assistance than orders made ancillary to the criminal process.

(2) In addition to a continuing examination of the issues identified in relation to breach notification, **other civil and penal remedies should also be examined, as those already developed in the various jurisdictions in their privacy legislations or otherwise.** Jurisdictions in Canada, the United States and elsewhere have enacted a broad range of other civil remedies including stipulating rights to free credit reports, credit freezes, and specified statutory damages for data breaches. The examination of civil remedies and approaches should focus first on areas that would provide the most benefit to victims of identity theft. Such areas would include remedies enabling prompt discovery of potential identity theft together with steps that may either lower the ultimate risk of that theft or mitigate the damage to credit history or other aspects of personal identity adversely affected.

(3) The Conference should consider an examination of steps that might be taken to enhance the security of personal information and to measures and practices that would reduce the risk of identity theft. Such preventive measures are a critical component of many legislative responses to identity theft.

[71] In light of these conclusions and in view of the benefits of broad participation and representation form several jurisdictions, the working group recommends that all jurisdictions participate in the following proposed ongoing work of the group:

(1) That the working group develop a principled framework for a breach notification scheme that could be used in all jurisdictions, together with an examination of related civil remedies and processes.

(2) That the working group conduct a detailed examination of remedies and processes to aid victims of identity theft where, criminal or other official records have erroneously been created in the name of the victim.

(3) That the long term objective of the group is to examine identity security, and what steps might be taken to enhance the security of identification documents and practices with a view to reducing the risks of identity theft.

---

1 The colloquial term "identity theft" is not without controversy. The working group recognizes that the term "theft" in this context may be thought inaccurate, raising as it does the notions of identity as property and of theft as deprivation. The victim of identity theft is not deprived of his or her identity, though he or she may lose money, time and reputation. However, "identity theft" is the common term, and it has been used in this report, subject to this caveat.

2 These statistics are available at http://www.phonebusters.com/english/statistics_E02.html

3 "Identity Theft – A Primer" from the Office of the Privacy Commissioner of Canada, available at http://www.privcom.gc.ca/id/primer_e.asp.

4 Identity Theft, *supra*

5 "Federal Trade Commission – Identity Theft Survey Report", Synovate Research, pages 9, 50

6 "Report on Identity Theft", Bi-National Working Group on Mass Marketing Fraud, October 2004, available at http://www.publicsafety.gc.ca/prg/le/bs/report-en.asp

7 "Working Together to Prevent Identity Theft: A Discussion Paper for Public Consultation", Consumer Measures Committee, page 2. Some of these difficulties may be addressed by an initiative proposed by Statistics Canada in "A Feasibility Report on Improving the Measurement of Fraud in Canada" available at http://www.statcan.ca/english/freepub/85-569-XIE/85-569-XIE2006001.htm

8 "First Estimates from the National Crime Victimization Survey: Identity Theft, 2004", Katrina Baum, Bureau of Justice Statistics, available at http://www.ojp.usdoj.gov/bjs/////pub/pdf/it04.pdf

9 FTC Releases Top 10 Consumer Fraud Complaint Categories, January 25, 2006, available at http://www.ftc.gov/opa/2006/01/topten.shtm

10 As summarized by the Privacy Rights Clearinghouse, updated February 2006, available at http://www.privacyrights.org/ar/idtheftsurveys.htm

11 A free version of the study is available at http://www.javelinstrategy.com/research/2. Some of the controversy surrounding these findings is summarized at http://blog.washingtonpost.com/thecheckout/2007/02/is_identity_theft_decreasing.html

12 "Identity Fraud: A Study", Cabinet Office, July 2002, available at http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf on

[13] Home Office Identity Fraud Steering Committee, available at http://www.identitytheft.org.uk/what-isbeing-done.htm
[14] "Updated Estimate of the Cost of Identity Fraud to the UK Economy", February 2006, available at http://www.identitytheft.org.uk/ID%20fraud%20table.pdf
[15] "How Serious is the Problem", CIFAS Online at http://www.cifas.org.uk/identity_fraud_is_theft_serious.asp
[16] "Fraud and Identity Theft", Parliament of New South Wales Australia Briefing Paper, Roza Lozusic, available at http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/08ACDBBA372ED89DCA256ECF0007C146
[17] "Fraud and Identity Theft", *supra,* See also "Report on Identity Theft", *supra*
[18] Report on Identity Theft", *supra*
[19] "Identity Theft: The Aftermath 2004", The Identity Theft Resource Center, page 12. Both the 2003 and 2004 reports are available at http://www.idtheftmostwanted.org/artman2/publish/lib_survey/index.shtml. It is not clear what impact legislated breach notification requirements may have on these figures.
[20] Identity Theft Survey Report, *supra,* at page 40
[21] Identity Theft: The Aftermath 2004, *supra* at pages 2, 13-14
[22] Identity Theft Survey Report, *supra,* at pages 6, 45-6
[23] Identity Theft: The Aftermath 2004, *supra* at page 14
[24] Identity Theft: The Aftermath 2004, *supra* at pages 8-9
[25] Identity Theft Survey Report, *supra,* at pages 6, 37
[26] Identity Theft Survey Report, *supra,* at pages 46-7
[27] Identity Theft: The Aftermath 2004, *supra* at pages 14-15
[28] Identity Theft Survey Report, *supra,* at pages 8,41-43, 45-6
[29] S. 54, *Criminal Law (Sentencing) Act 1988*
[30] The underlying rationale for the certificates is described in "Discussion Paper: Identity Crime", Model Criminal Law Officers Committee, page 28. This document is available at http://www.justice.tas.gov.au/__data/assets/word_doc/78609/Identity_Crime_Discussion_Paper.DOC

[31] This limitation has also been noted by other observers. See for example South Australian Laws Target Identity Theft", Jeremy Douglas Steward, [2004] Privacy Law and Policy Reporter 8, available at http://www.austlii.edu.au//cgi-bin/disp.pl/au/journals/PLPR/2004/8.html?query=identity%20theft
[32] Discussion Paper, *supra,* at page 28
[33] "Review of the Legal Status and Rights of Victims of Identity Theft in Australia", James Blindell, Australian Centre for Policing Research, 2006.
[34] Michigan Senate Bill 794, available online at http://www.legislature.mi.gov/(S(jh22nhnfwzfnxv55jlvhts45))/mileg.aspx?page=getObject&objectName=2003-SB-0794
[35] The nature, scope and function of these provisions is described in documents available from the Office of Privacy Protection within the California Department of Consumer Affairs. An overview is provided in "How to Use the California Identity Theft Registry: A Guide for Victims of "Criminal" Identity Theft", available at http://www.privacy.ca.gov/cover/identitytheft.htm
[36] California Penal Code 530.6, 851 .8(a)-(d)
[37] California Penal Code 851.8(h)
[38] California Penal Code 530.7
[39] Minnesota HF 1943, Session 84, Wyoming Senate File SF0053, Arizona HB 2716
[40] Ill. Comp. Stat. § 5/16G-30; 2005, N.C. ALS 414, Conn. Gen. Stat. § 54-93a.,
[41] ***R. v. Zelensky*** [1978] CarswellMan 51 at paragraph 4 (S.C.C.)at paragraph 33
[42] ***Zelenski,*** *supra,* at paragraph 34. A further example may be found in the inability to use these provisions to recoup opportunity costs rather than more direct losses – ***R. v. Brunner*** (1995) 97 C.C.C. (3d) 31 (Alta. C.A.)
[43] ***Zelenski,*** *supra,* at paragraph 28
[44] See for example the Consumer Identity Theft Kit produced by the Consumer Measures Committee Working Group on Identity Theft, available at http://cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00084e.html

[45] See the National Conference of State Legislatures' web page on Breach of Information for links to legislation and related resources, at http://www.ncsl.org/programs/lis/cip/priv/breach.htm , and the appendix to the CIPPIC study, below, note 47.
[46] S.O. 2004, c.3, Sch. A, s. 12(2). Online: http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm
[47] See in particular Canadian Internet Policy and Public Interest Centre (CIPPIC), "Approaches to Security Breach Notification: A White Paper", January 9, 2007, http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-web.pdf
[48] Information and Privacy Commissioner (Ontario), "Safeguarding Privacy in a Mobile Workplace: Protect the Information you keep on your laptops, cellphones and PDAs" (June 2007) http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf. See also "Fact Sheet: Encrypting Personal Health Information on Mobile Devices", May 2007, http://www.ipc.on.ca/images/Resources/up1fact_12_e.pdf .
[49] S.C. 2000 c.5, Part 1. The report is online: http://cmte.parl.gc.ca/cmte/CommitteePublication.aspx?SourceId=204322.
[50] The Committee heard of a B.C. case where the data improperly released was health information of mental illness patients in an institution. The B.C. Commissioner needed to consider the impact of disclosure on these vulnerable individuals. (Proceedings for December 6, 2006.)
[51] On identity theft in general: http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html (also found at http://www.consumer.gov/idtheft); for people whose information may have been compromised. "If your information has been compromised, but not yet misused", http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/compromised.html; and for businesses, "Information Compromise and the Risk of Identity Theft: Guidance for Your Business", http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm.
[52] California Office of Privacy Protection, February 2007, "Recommended Practices on Notice of Security Breach Involving Personal Information", http://www.privacy.ca.gov/recommendations/secbreach.pdf
[53] Privacy Commissioner of Canada, "Businesses and Identity Theft", March 2007, http://www.privcom.gc.ca/id/business_e.asp.
[54] December 2006, http://www.oipcbc.org/pdfs/Policy/ipc_bc_ont_breach.pdf
[55] See the complete list at http://www.oipcbc.org/sector_private/resources/index.htm
[56] "What to do if a privacy breach occurs: Guidelines for government organizations", http://www.ipc.on.ca/images/Resources/up-prbreach.pdf . A similar document was published for organizations with health information, "What to do when faced with a privacy breach: guidelines for the health care sector", http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf
[57] David Loukidelis, testimony before Committee, November 29, 2006
[58] Information and Privacy Commissioner (Ontario), "Do the right thing, Ontario, make a move now to fight ID theft", News Release, February 6, 2007, http://www.ipc.on.ca/images/Resources/up-2007_02_06_idtheft.pdf
[59] Public Interest Advocacy Centre (PIAC), "Canadian Consumer Initiative Identity Theft Policy Position", February 2005, ,http://www.piac.ca/financial/canadian _consumer _initiative _identity _theft_policy_position
[60] CIPPIC, above, note 47.
[61] Consumer Measures Committee, July 2005, http://cmcweb.ca/epic/site/cmc-cmc.nsf/vwapj/Discussion%20Paper_IDTheft.pdf/$FILE/Discussion%20Paper_IDTheft.pdf. See the CMC's general identity theft resources for consumers and businesses at http://cmcweb.ca/epic/site/cmccmc.nsf/en/fe00084e.html .