UNIFORM LAW CONFERENCE OF CANADA

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

Readers are cautioned that the ideas or conclusions set forth in this paper, including any proposed statutory language and any comments or recommendations, have not been adopted by the Uniform Law Conference of Canada. They do not necessarily reflect the views of the Conference and its Delegates.

Quebec City
August 2008

Report of the Working Group
August 2008

Introduction

[1] Identity theft, or usurpation of identity, is a significant problem giving rise to complex problems for individuals, governments, and the justice system. In 2006, a joint civil / criminal working group was formed to examine some of these issues. The group presented its first report to the Conference in 2007. As a result of that report, the following resolution was passed:

> *1. That the Joint Criminal/Civil Section Working Group on Identity Theft:*
> *(a) 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; and*
> *(b) 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.*

[2] These two issues are addressed in the Report that follows.

[3] The working group is comprised of the following members:

(1) Josh Hawkes – Appellate Counsel, Alberta Justice
(2) John Gregory – General Counsel, Policy Division, Ontario
(3) Jeanne Proulx – Counsel, Legislative Draftsperson, Quebec
(4) Wilma Hovius – Counsel, Public Law Policy, Justice Canada
(5) Erin Winocur – Counsel, Criminal Law Policy Branch, Ontario
(6) Gail Mildren – General Counsel, Civil Legal Services, Manitoba Justice
(7) Lynne Kohm – Senior Crown Attorney, Policy Development & Analysis Division, Manitoba Justice
(8) Joe Pendleton – Director, Special Investigations Unit, Alberta Solicitor General

Privacy Breach Notification: Options for a Principled Framework

[4] At the 2007 meeting of the Uniform Law Conference of Canada, the Working Group on Identity Theft submitted a discussion paper on diverse aspects of identity theft, including a section on laws that require holders of personal information to report to the individuals whose personal information has been stolen, lost or otherwise compromised.[1] The purpose of requiring notice of a privacy breach is to help people to protect themselves against the misuse of their personal information once it has been disclosed beyond what they have consented to or could reasonably expect.

[5] A joint meeting of the Criminal and Civil Sections of the Conference resolved at that meeting, among other things,[2] "that the Joint Criminal/Civil Section Working Group on Identity Theft …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 …"

[6] The present document responds to that resolution: it presents options for a principled framework for a breach notification scheme. It does so under a number of separate headings:

a. What information is covered by the breach notification scheme?
b. What holders of information are covered?
c. What is a "breach" or compromise?
d. When is a breach or compromise reportable?
e. Who decides if a breach has occurred and is reportable?
f. What is the response to a breach?
g. What does the notice of breach say?
h. How are these obligations enforced?
i. What else should be included in the framework?
j. What form should uniform legislation take?

a) What information is covered by the breach notification scheme?

[7] There seems little controversy that what is covered is personal information in the hands of the holder of that information. Ideally, enacting jurisdictions would define personal information for the purposes of breach notification as it is defined in the statutes that govern its protection. Any breach notification legislation should be drafted in a way that can be inserted into the privacy legislation itself.

[8] Some jurisdictions may have different definitions for different purposes. For example, all provinces have legislation that protects the privacy of personal information in the public sector, but only three have legislation that protects it generally in the private sector. Thus commercial use of personal information in the other seven provinces and three territories depends on the federal legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA may define personal information differently than the public sector legislation. The three provinces with their own private-sector legislation have been found

substantially similar to PIPEDA in their operations, but if their definition of personal information is not identical, the same issue arises.

[9] It appears in practice, however, that the definition of personal information in all Canadian information privacy legislation has a common core: information about an identifiable individual. There is some variation on whether that information must be 'recorded' in order for the legislation to apply. The principles discussed in this paper are assumed to apply across the country without regard to any differences in statutory definition.

[10] Again, some provinces have separate legislation to protect personal health information. Aside from the definition questions, should personal health information be covered by the breach notification policy? Is there anything about the custodians or trustees of personal health information that makes the policy harder or less appropriate to apply to them? These custodians or trustees can be public sector bodies, like government departments and most hospitals, or private bodies like laboratories, or semi-public bodies like some clinics. Medical practitioners are mostly in the private sector as well. Their information storage capacity may be quite diverse across a province and across the country. Likewise their potential to analyse breaches and to notify the persons affected may vary greatly. However, such variations are best addressed through substantive rules, and not by depriving people of protection because of the nature of the holder of their information.

[11] **Recommendation**: The breach notification scheme should apply to all kinds of personal information protected by the laws of the enacting jurisdiction.[3]

b) What holders of information are covered?

[12] The answer to this question has been anticipated in the previous discussion. The people whose information has been compromised need the same protection regardless of who was holding the information at the time. There may be issues about the form of the legislation as applicable to different groups of holders, a topic dealt with later in this paper.

[13] **Recommendation:** The policy should apply to all holders of personal information who are subject to information privacy laws in the enacting jurisdiction.

c) What is a "breach" or compromise?

[14] Answering this question requires us to look beyond the requirements of the applicable legislation respecting the security of personal information. All such legislation puts some onus on the holder of personal information to take care of it, though not usually with much specific behavioural direction.[4] Sometimes private standards may apply as well. The best known are the Payment Card Industry (PCI) data security standards, devised by the major credit card issuers.[5] Likewise, privacy commissioners have proposed best practices for security measures.[6] However, even if the statutory, regulatory or industry standards have been complied with, it is possible that personal information will be lost, stolen or compromised. After all, the need of the data subjects to protect themselves does not depend on the care with which the information was protected before it was lost, stolen or compromised.[7]

[15] It is not the task of the Uniform Law Conference to prepare information security standards to protect privacy. It is possible, however, to consider the major methods by which personal information can be compromised, based either on basic principles of information management or on reports of data breaches that have come to public attention.[8] This list is only an indication of the range of possibilities.

- Physical breach: the computer(s) containing the data were in a locked room. The lock was broken and the computers are gone.
- Physical breach: the computer(s) containing the data were in a locked room. The lock was broken but the computers are still there. It is (not) possible to tell if the information was accessed.
- Physical breach: the computer(s) containing the data were in a locked room, but the lock was left unlocked over a period when someone outside the organization might have got in.
- Physical breach: a mobile computer containing personal information is stolen, either from the office or from a car or the home of an employee.
    a. The laptop is never recovered.
    b. The laptop is recovered but it is (not) possible to tell if the information was accessed.

c. The information on the laptop was protected in some way:
   i. It was in a password-protected file
   ii. It was encrypted (by a more or less reliable method)
   iii. It was anonymized or otherwise de-linked to individuals

- Virtual breach: an electronic means of access to the personal information was not secure against unauthorized access, from inside the organization or from outside.
- Virtual breach: an electronic means of access to the personal information was not secure against unauthorized access, from inside the organization or from outside, and there is evidence of actual unauthorized access.
- Virtual breach: an electronic means of access to the personal information was penetrated by hackers using a known vulnerability of the system.
- Virtual breach: an electronic means of access to the personal information was penetrated by hackers using a new, previously unknown vulnerability of the system.

[16] The purpose of notification of a breach is to enable people to take steps to protect themselves against a misuse of their personal information. Thus the risk of misuse is an important element of the need for notification. While insufficiently protecting personal information may be a breach of the relevant statute (though as noted, most such statutes are not very precise on the standard of care), it is arguable that a duty to notify should arise only when there is a serious risk that someone has in fact accessed the data. The existence of an opportunity is not enough. However, how long an opportunity has existed may affect the duty. For example, if a website allowed access to personal information for six months, that is a more serious compromise than if the vulnerability lasted a weekend.

[17] The guidelines for notification of breach published by the Privacy Commissioner of Canada speak of a stolen laptop with "adequately encrypted information". If the laptop is recovered and analysis shows that the information was not tampered with, then the Privacy Commissioner's document suggests that no notification would be needed.[9]

[18] The breach we are talking about is one that leads to improper access to or disclosure of personal information. Breaches of the duties of appropriate collection and use of such information by the data holder are not covered in this paper.[10] After all, the point of disclosure

of a breach is to allow people to protect themselves against abuse of the information in unforeseen hands. It is irrelevant to this purpose that the data holder itself may have collected too much information or that it may be using the information for unexpected purposes.

[19] **Recommendation:** The policy should apply to breaches of information security that present actual knowledge or a reasonable risk that personal information has been improperly accessed or disclosed.

d) When is the breach or compromise reportable?

[20] Even if there has been a breach that presents a reasonable risk that personal information has been improperly accessed or disclosed, it may be that it does not need to be reported. This is the key question: when will the requirement to notify of a privacy breach apply? The purpose of breach notification is to reduce the harm done to people by the disclosure of their personal information beyond what they have consented to or could reasonably expect. When does this need for protection arise? What criteria might be applied to decide? For example:

- The vulnerability of the information: if the information were encrypted with strong encryption, then the person who has stolen or accessed it probably will be unable to misuse it.
- The number of people whose information is at issue: are a hundred people affected, a thousand, a million?
- The sensitivity of the information or its importance to the persons it is about: is the information about their shopping habits, their educational results, their financial status or their health?

[21] To evaluate properly the risk of harm, it may help to consider the nature of the harm that may be suffered. What is the risk or threat to the individual of unauthorized disclosure of his or her personal information? Risks include physical harm, including through harassment or stalking, identity theft, financial loss, the loss of business or employment opportunities, and humiliation, damage to reputation and relationships, for example through loss of information in mental health or other medical records or disciplinary records.[11] There is a well-organized black market for credit card information,[12] so the risk from compromise of financial information must

be taken seriously. It can also be dangerous to one's health if someone else actually uses one's health information for the thief's own treatment purposes.[13]

[22] No single factor seems likely to gauge the need of people for protection. A combination of factors will be needed, and even then, the number of people affected seems unlikely to be relevant. If highly sensitive information was improperly released about one person, should not the law require that the data holder inform that person of the threat to his or her information?

[23] Notification is not free, however. There are two kinds of cost to the process. The first are the costs to the data holder in giving the notice, which must include the market (reputational) costs that will follow public knowledge that the holder has lost the data. The latter aspect may be heavier than the costs of postage or administration of the notification. There may also be civil liability for the harm done by the breach, though to date no case in the United States or Canada has resulted in judgment for the plaintiff.[14] The second kind of cost is the cost to the individuals who receive notice: they may have financial outlays in checking their credit ratings and in repairing or redoing their financial arrangements to avoid or make good the losses. They may also have a psychological cost in worry whether any actual harm will come of the disclosure of the information, or concern for the embarrassment if some of the information becomes known to those whose opinion is important to them.[15]

[24] As a result, a balance is needed between notification in all cases and under-notification. This balance will depend to some extent on whether the costs to the data holder are given much weight when compared to the interests of the individuals affected by the breach in protecting themselves. One may wish to tie the imposition of these costs to whether the data holder was at fault in the breach, but the data subjects' need for protection does not depend on the cause of the breach.

[25] It is conceivable in some circumstances that a contract could be made between the individual the information is about and the data holder, requiring notification under conditions set out in the contract. However, in many circumstances no contract would be possible, either because the information was collected from someone other than the individual it is about, or because it was collected with an "opt-out" consent. It would be awkward to impose a contract when all the individual was being asked is whether he or she objects to the collection and use of

personal information. In law an "opt-out" consent to a contract is possible, but it is not clear that such a legal relationship would be clearer or more desirable than a legislated rule that would apply to everyone, whether or not bound by contract.

[26] The Privacy Commissioner of Canada proposes that notification be given "[i]f a privacy breach creates a risk of harm to the individual".[16] She goes on to give a list of factors, including "risk of harm to the individual, ... reasonable risk of identity theft or fraud, ... risk of physical harm, ...risk of humiliation or damage to the individual's reputation" and the individual's ability to avoid or mitigate the harm.[17] Her Ontario counterpart suggests that notice should be given in every case,[18] though her collaboration with the British Columbia Commissioner set out below suggests more nuance. In British Columbia the official advice is that "notification can be an important mitigation strategy in the right circumstances."[19] The B.C. Commissioner, along with the Ontario Commissioner, have published a "breach notification assessment tool" to help decide when and how to notify individuals.[20] That document speaks of the risk of identity theft and asks "how reasonable is the risk?" It also asks about risk of physical harm, risk of hurt or humiliation, and risk of loss of business or employment opportunities. In short, there is a good deal of overlap among the commissioners in Canada.

[27] It is a common theme in the writing on the topic that the need to notify people of a privacy breach should reflect their need for protection from the consequences of the breach. Thus the certainty that there has been a breach at all combines with the threat apparently presented by the type of breach (e.g. unauthorized access, theft of hardware, direct attack on data) and the sensitivity of the information and the potential harm that can be done by its being in the wrong hands. It is not possible to put a numerical weight on these factors, so estimating the importance of notice is not a mathematical or exact calculation. It is always a matter of judgment, and each case will be unique.

[28] The range of possible calculations can be indicated in five options. The wording is important, though not magical, i.e. the words are intended to indicate a policy choice, not to be applied automatically. The five options are expressed in increasing obligation to give notice of the breach. The degree of fault of the data holder with respect to the breach is not relevant to the

need for notice and thus to the obligation to disclose the breach, even though mandatory disclosure may feel like a kind of penalty to the data holder.

a. A privacy breach must be disclosed to the people whose information has been compromised if the benefit of disclosure to those individuals outweighs the cost of disclosure to the data holder (bearing in mind the potential negative aspects of disclosure to the individuals as well.)
b. A privacy breach must be disclosed to the people whose information has been compromised if there is a substantial risk of serious harm to those individuals as a result of the breach.[21]
c. A privacy breach must be disclosed to the people whose information has been compromised if there is a risk of significant harm to those individuals as a result of the breach.[22]
d. A privacy breach must be disclosed to the people whose information has been compromised if there is a risk of misuse of the personal information according to relevant legislative standards.[23]
e. A privacy breach must be disclosed to the people whose information has been compromised unless exceptional circumstances make it undesirable in the particular case.

[29] **Recommendation:** A privacy breach must be disclosed to the people whose information has been compromised if there is a risk of significant harm to those individuals as a result of the breach.

e) Who decides if a breach has occurred and is reportable?

[30] In the first instance it will almost always be the data holder that finds out about the breach of information security. Does the data holder get to make the decision about whether the compromise to security constitutes a breach subject to the rules, and whether to disclose this breach, i.e. to apply the test for disclosure set out in the previous discussion? The data holder will have the best knowledge at the outset of the type of information involved and the nature of the individuals to whom the information relates. Thus it is in a good position to make the judgment – except that the data holder also has strong incentives to avoid disclosing the breach. The consequences of disclosure are likely to be unpleasant for it. There will be substantial costs

in sending out notices. Sometimes the information may not include addresses of the individuals the information is about, and the business of the data holder may not include regular communication with them, so a whole separate process will have to be created to send the notices. Usually there will be bad publicity as a result, which can hurt the sale of the data holder's goods and services and also the price of the shares if the holder is a public company.

[31] This disincentive is one reason to make the test for identifying a breach and disclosing it as automatic or as easy to apply as possible. The more general words of quality – like "substantial" risk or "significant" harm – the easier it is for the data holder to decide that a particular breach is not covered by the obligation to disclose.

[32] The main alternative to leaving the data holder to decide whether to disclose is to give the decision to the authority responsible for enforcement of information privacy legislation in the jurisdiction. It was proposed above to define breach with reference to a particular statute, and all the relevant statutes make some provision for their enforcement. Public sector breaches would be referred to the independent review officer that oversees public sector privacy compliance: at the federal level, to the Privacy Commissioner of Canada; in Ontario, to the Information and Privacy Commissioner; in Manitoba, to the Ombudsman; etc. (Solely for convenience, the term "commissioner" is sometimes used in this paper to cover all such review officers.) Private sector breaches would be referred to the provincial commissioner where provincial private-sector legislation applies, and otherwise to the Privacy Commissioner of Canada if there were a breach of PIPEDA. The commissioner would investigate the circumstances with the data holder and would decide whether notification was desirable or not.

[33] The standard for disclosing the breach to the commissioner would be lower than for disclosing it to the people affected by the breach, or to the public at large, since the commissioner can balance the equities and the risks in further disclosure, instead of the data holder having to do so. The commissioner would apply the standard stated above for disclosure to the individuals the information is about. The point of letting the commissioner make the decision is to get a more objective decision on that point.

[34] Even a duty to refer a breach to the commissioner leaves the decision with the data holder whether there has been a breach at all. The mere opportunity for unauthorized access may not be

considered a breach – though if one has lost the storage medium entirely (like a laptop or a hard drive), then there should be at least a presumption of such access. This consideration pushes for a clear and precise definition of breach and a broad obligation to report to the commissioner, even if the obligation to notify individuals is narrower. The main penalty for covering up may be increased embarrassment if the breach is discovered later, though other sanctions may be available too.[24]

[35] One might wonder whether there should be a kind of reciprocal relationship between the standard for disclosure and who gets to decide. The higher the threshold for deciding, the less it should be the data holder who decides, because of that entity's interest in not reporting. If breaches are less serious, then the data holder can decide, and if that decision is self-serving, then it does not matter so much. However, the rule will have to apply to all breaches, not just breaches of a certain magnitude, since the question of magnitude is at issue here. If one ever leaves the decision to the data holder, then one leaves it there for all manner of breaches. So this dichotomy does not work well when analysed further.

[36] In some cases unauthorized access to data will constitute a criminal offence, and of course where a computer has been stolen, there is a criminal offence. There is sometimes a tension between the need to give prompt notice to individuals that they may be at risk because of a privacy breach and the need to allow the police to investigate without arousing suspicion. It is arguable that there should be a duty to notify police in cases that do raise criminal issues, whether this duty should be on the data holder or on the privacy commissioner when the commissioner is notified.[25] (Probably if there was not enough of a breach to notify the commissioner, then there was not enough to notify the police.)

[37] Besides notification to affected individuals and the police, legislation might require the maintenance of a public data base of compromises of security. The Canadian Internet Policy and Public Interest Clinic (CIPPIC) recommended that the Privacy Commissioner of Canada should set up such a data base, and that all breaches, however slight, should appear in it.[26] This would serve as an additional incentive for data holders to be prudent, to stay out of the data base, and also provide a useful overview of the state of data security in the relevant jurisdiction. CIPPIC was addressing only PIPEDA so did not address whether a single national data base could be

assembled from all jurisdictions. The working group is not now recommending such a data base but is open to the views of the Conference on whether it should be made mandatory and if so, with respect to what level of breach.

[38] **Recommendation:** The data holder should have to notify the relevant privacy commissioner or privacy review officer of any breach involving unauthorized disclosure of or access to personal information.[27] The commissioner or officer should have the power to require the data holder to notify individuals if the statutory test for notice is met. The commissioner or officer should also be required to notify the police where circumstances warrant.

f) What is the response to the breach?

[39] The typical response to the breach will be disclosure of the breach to the individuals affected by it. The advice offered by privacy commissioners and privacy review officers – and they appear unanimous on the point – is that a proper response to a breach must include analysis of the cause of the breach, action to make it stop as soon as possible, possible reporting to the police if some illegality appears to have been involved, and in the longer term, action to avoid the repetition of the breach in the future. None of these topics other than disclosure of the breach seems appropriate for legislation. Failure to stop the breach will of course risk continued access to personal information, and an increasing number of notifications to send. As a matter of public relations, the data holder would want to be able to say what it has done to put an end to the problem. The timing of remedial action or disclosure may await the advice of the police, if they need to investigate how the breach occurred first.

[40] Again, the privacy commissioner or review officer can advise – and if the data holder is to be left to decide, then it will have to do so, and the law should perhaps provide guidance – on how to give notice of the breach. Will individual contacts be required – by phone or mail or e-mail? Will bulk notice via the media be appropriate for very large groups, or for groups for which the data holder does not have addresses?

[41] **Recommendation:** Do not provide any rules about how data holders should respond to the breach except as they relate to giving notice of the breach.

g) What does the notice of breach say?

[42] The basic language of the notice is not in doubt: the personal information of the person receiving the notice has been compromised. Presumably the notice also gives the best information available as to the scope of the information involved, and the time and circumstances of the breach. The notice in other words gives the individual the most information that will allow them to protect themselves against the harmful consequences of the breach (some of which were listed earlier.[28]) Should the law require the notice to present this information in any specific way? Or will the data holder be led by general duty to find an effective way, the failure to do which is a matter for enforcement later?

[43] A more open question is whether the notice should contain more information about the rights of the data subject, or advice on how to protect one's rights or interests while one's personal information is at large. The privacy commissioners' guidelines referred to earlier give an array of possible texts, either in general or as draft language. Some of the topics are:

- Advice to find out one's credit rating and an explanation of how to do so.
- Information on rights to a credit freeze (so no one can get credit in one's name without express authorization) or other remedies.[29]
- Information on how to change a health card number, Social Insurance Number or driver's licence number.
- Contact information at the data holder's organization, for more information.
- Contact information for the relevant privacy commissioner or review officer, for more information and possible filing of a complaint about the breach.
- Other sources of information about how to protect oneself in such circumstances, such as Industry Canada's site or the sites of privacy commissioners.[30]

[44] **Recommendation:** If the policy choice is to require data holders to disclose breaches to the privacy commissioners and review officers and follow their advice, then the legislation does not need to spell out the content of the notices. That will be a matter for the commissioner or review officer and the data holder. If the decision on disclosure is left to the data holder, then the statute should give a recommendation on the content of the notices, at least in generic terms.

h) How are these obligations enforced?

[45] Three routes are available to enforce the obligations in the new legislation: civil, regulatory and criminal. A civil remedy would be a lawsuit between the data subject whose information has been compromised, and the data holder. Normally lawsuits would not need special authority in the statute, whether an individual or a class proceeding were in prospect. The only reason to consider otherwise here is that the experience in the United States has been that civil plaintiffs have been widely unable to recover in such actions. The problem has been that they have not been able to link any specific damages to the improper disclosure of their information. In most cases the plaintiffs have not suffered any damage, but it is also hard to link particular damage to a particular disclosure, even if identity usurpation has occurred. The best people have done so far is to recover costs for their credit checks.[31] Sometimes the companies giving notice will cover those costs voluntarily, as a matter of good public relations.

[46] It would be possible to provide by statute a right to statutory damages in a successful civil suit. That would avoid the need for proof of actual harm from the breach. It would also strengthen the deterrent effect of the law, or rather the incentive effect on data holders to guard the information carefully. Arguably statutory damages should apply only in cases where the data holder is found at fault, and not where the breach was unavoidable by taking reasonable care. It could be a challenge, however, to set the amount of statutory damages in a way that would be fair to all parties in cases where only a few people are affected and in cases with many thousands or even millions of potential plaintiffs. It may be more useful to provide substantive remedies, rather than an amount of cash that is bound to be arbitrary.[32]

[47] Regulatory enforcement would be in the hands of the privacy commissioners and review officers. Such enforcement could include a simple order to make disclosure or a more detailed order prescribing the wording or manner of the disclosure or even the imposition of penalties for failure to report a breach to the commissioner or review officer or for non-compliance with previous orders. It should be noted, however, that only a few commissioners have the power to make orders under their current legislation. Some commissioners and review officers make recommendations only, with powers similar to those of an ombudsman. The decisions of the Privacy Commissioner of Canada under PIPEDA are subject to enforcement in some circumstances in the Federal Court, but only the court's order has force of law. In the alternative,

the Conference could leave the issue of orders to the enacting jurisdiction to decide: does it want to remain consistent with the rest of its privacy legislation with respect to oversight? Governments may be very reluctant to increase the power of their commissioners so drastically.

[48] Administrative penalties – i.e. fines imposed directly by a regulatory authority, without a conviction in a court – have developed in Canada and elsewhere in recent years. They have been upheld in the courts if they have been subject to some degree of judicial review. Thus the commissioner would not be the order-maker, prosecutor and final judge all in one. However, the power to impose such penalties is an even larger step away from the mediative or facilitative role of many of the commissioners or review officers than the making of orders. An additional consideration makes such penalties doubtful for non-compliance by public bodies: privacy commissioners and their counterparts are frequently officers of the Legislature (or of Parliament, in the case of the federal government). It may not be appropriate for such officers to take money from the Crown in penalties – but if the penalties are paid into consolidated revenue, then it is merely going from one pocket to another.

[49] Criminal or quasi-criminal enforcement would probably apply only to serious infractions of the responsibilities under the notification laws. Rather than give privacy commissioners and review officers the power to make orders (or in addition to doing so), jurisdictions could create an offence of non-compliance with the notification requirements in the legislation. (If other criminal activity were at issue, then the usual criminal laws would apply, of course.) Prosecution may be a useful alternative to regulatory action in jurisdictions where the regulator cannot directly make orders or where legislators do not want to give commissioners the power to impose penalties. Such proceedings may be undertaken by Crown prosecutors if privacy commissioners or their counterparts were not comfortable doing so. Some discussion would be advisable between the potential participants before a jurisdiction prepared legislation on the topic.

[50] It would be possible to provide expressly the degree of liability for a new offence, if that were desired. For example, breach of an obligation to notify, or of an obligation to comply with an order of the privacy commissioner or review officer respecting breach notification, could be expressly made a strict liability offence, so that the non-compliant person would have to demonstrate due diligence in order to avoid conviction.

[51] Enforcement of the obligation to give notice of a privacy breach is separate from a potential prosecution for failure to keep the data secure in the first place, as (usually) required in privacy legislation now. Some instances of breach may support the latter kind of prosecution, even if notice of the breach has been given to affected individuals. In the United Kingdom the Privacy Commissioner has recently been given the power to fine organizations if their operational procedures cause a gross breach of data protection principles. This is an administrative penalty imposed for not keeping information secure, rather than for not reporting incidents of insecurity.[33]

[52] **Recommendation:** Create an offence of failing to notify as required, and of failing to comply with an order of the commissioner or review officer, where that official has the power to give orders. Jurisdictions are invited to consider giving order-making powers for these particular offences, even if such powers do not exist elsewhere in the privacy statute. The commissioners or their counterparts should have primary but not exclusive responsibility for investigating whether information holders have complied with the statutory obligations. The Working Group makes no recommendation about who should take the initiative to prosecute; each enacting jurisdiction must decide what makes most sense in the context of its privacy regime. Do not bar civil remedies, but do not create statutory damages for failure to notify of a breach of information security.

i) What else should be included in the framework?

[53] The purpose underlying this set of proposals is to protect individuals whose personal information is disclosed in violation of privacy legislation. Giving those individuals notice of the unauthorized disclosure is the first step, but it may not get them very far. In particular, the threat of identity theft or usurpation hangs over the heads of these individuals, depending for its severity on the nature of the information improperly disclosed. It is a general recommendation in these cases that people should check their credit ratings. However, this can be administratively difficult, time-consuming and expensive. Legislation could facilitate the process by giving individuals rights to access their credit rating files cheaply. Some US legislation requires a certain number of free access requests.[34] It also requires that the three large credit-rating agencies in the US cooperate with each other, so that an individual's request to one agency for

information is passed on by that agency to the others, so the person gets information from all three for the one request.[35]

[54] In addition, just checking from time to time may appear a weak remedy – indeed no remedy, just an alert to problems that one will have to resolve if the check turns up a problem.[36] Some US states have provided for a voluntary credit freeze, by which the person at risk ensures that no one can open up an account based on credit without special secure contact being made with the person. In other words, the data thief will not be able to use the stolen information alone to get credit.[37] Of course that makes it somewhat harder for the genuine person to get credit too, but that may be considered an acceptable trade-off. The credit rating agencies find this kind of provision an imposition.[38] If a fee were to be charged, the amount might be assigned to the data holder whose breach has caused the need for the freeze.

[55] It is also unclear how effective such measures are at blocking unauthorized use of identity. In any case, a credit freeze can prevent only an abuse of credit. Other misuses of a usurped identity, such as in transactions or criminal activity, are not caught by such a measure. That a measure may cure only some of the harm is not an argument for doing nothing.

[56] One could comb through the legislation in the United States, where at least 40 jurisdictions have enacted (often inconsistent) breach notification statutes, for further constructive ideas to supplement the basic notification rule.[39] Any Canadian legislation would be provincial or territorial legislation, to regulate an industry under provincial power. Attention would be needed to co-ordinate the cross-jurisdictional issue, given that the agencies have a head office somewhere but carry on business across the country. As part of legislation aimed at the credit reporting agencies, a uniform statute could regulate the agencies' fees for these services, or allocate the fees to the person responsible for the breach – whether or not there is fault on the part of that person.

[57] **Recommendation:** Provide for cooperation by credit reporting agencies in responding to requests. Do not provide for a mandatory credit freeze without more evidence of its likely effectiveness.

j) What form should uniform legislation take?

[58] As noted earlier, all provinces and territories have public-sector privacy legislation. Some have legislation specific to personal health information that applies to all or part of the public sector and to parts of the private sector. A few provinces have general private-sector privacy legislation. The federal government has public-sector legislation and private-sector legislation that applies to commercial activity across the country, except where displaced by provincial legislation. Uniform legislation on breach notification should be able operate with all of them, since the Conference will probably recommend enactment to all.

[59] There are two main options:

a. Draft legislation in a form that can be inserted directly into the existing privacy legislation of the enacting jurisdiction; or
b. Draft a free-standing statute that could be enacted on its own, to impose this obligation on entities even if they are not otherwise covered by provincial or territorial privacy legislation.

[60] The advantages of option (a) are simplicity and a respect for the policy decisions of the jurisdiction on legislating on privacy. The disadvantages are that some groups of provincial residents may not have the protection of notification of unauthorized access to their information.

[61] The advantages of option (b) are universality: everyone benefits from breach notification, even if other obligations of the private sector are not spelled out in legislation. One would have to draft this legislation to incorporate the privacy-protection standards whose breach would call the statute into play, since one could not simply refer to a breach of the existing statutory rule. On the other hand there could be some awkwardness in a province to which PIPEDA applied, if the federal statute is given a breach notification rule different from what is to be applied in the province or territory. However, provincial or territorial law could impose a notification duty on holders of personal information not covered by PIPEDA, such as employment information or information not collected, used or disclosed for a commercial purpose.[40]

[62] **Recommendation:** Draft uniform legislation to fit into each enacting jurisdiction's existing privacy legislation.

Conclusion

[63] The Working Group on Identity Theft recommends legislation to make notification of privacy breaches mandatory in significant instances, using the jurisdictions' privacy commissioners or independent privacy review officers as the screens for the important decision whether the breach is important enough to justify the costs to all parties of notification. At this time the Working Group does not recommend more detailed legislation about other elements of data breach, such as prescriptions for post facto repair of reputations or express civil remedies, beyond the creation of an offence for failing to comply with the primary obligations of the statute.

[64] One may ask, however, whether legislation is needed at all. Why not stop at a statement of the applicable principles, as set out in this report (or as amended by resolution of the Conference), leaving each province and territory to legislate on its own? The Working Group's answer is twofold:

a. First, this would get us little further than where we are now, since the privacy commissioners and review officers who have written on the issue are in close accord on the principles. The point of the Conference's work is to give all jurisdictions a voice in refining those principles, so that adds some value, but the practical impact may be little different.

b. Second, it is important for data holders that carry on activities in more than one Canadian jurisdiction to have a predictable and ideally uniform obligation to their data subjects across the country. Arguably public-sector entities have less need for national consistency, since the people whose information they hold are generally within the single jurisdiction, and if the laws are somewhat different than across the provincial or territorial border, the inconvenience may be slight. This is not true for organizations that operate in multiple jurisdictions. The only way to provide uniformity, or even harmony, with sufficient certainty is to legislate in the same way.

[65] The Working Group recognizes that uniform statutes are not necessarily enacted word for word across the country. In particular, Quebec often finds a distinct way to legislate, because of

the features of its Civil Code or otherwise. Nevertheless the shared goal of finding a national principle and having it apply nationally is best attained from a common base of a uniform statute.

Identity Theft – Victim Assistance Options for Erroneous Criminal Justice Records

[66] The term "criminal identity theft" is frequently used to refer to situations in which the perpetrator uses the name of an innocent victim, either alone or in combination with other identity documents, in dealings with law enforcement and others in the criminal justice system. Such encounters give rise to erroneous documentation, orders and records that put the victim at risk of arrest or other official sanction. The State of California 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.[41]

[67] In 2005, the U.S. Department of Justice and the Bureau of Justice Statistics convened a national focus group on identity theft and criminal record repositories. The report of this focus group provides a useful delineation of three ways in which identity theft, or identity mistakes can occur resulting in errors in criminal record databases:

a. **Intentional Identity Theft –** when an individual deliberately uses the name or identification of another in order to avoid arrest or otherwise frustrate a law enforcement investigation.

b. **Inadvertent Identity Theft –** when an individual provides a fictitious name or identity that **coincidentally** belongs to or closely resembles that of an actual person in order to avoid arrest or otherwise frustrate a law enforcement investigation.

c. **Non-Theft Identity Mistakes –** when an individual provides their true name, but it is **identical** or closely related to, and mistakenly associated with an innocent person's identity.[42]

[68] A criminal or other official record may erroneously be created in the name of the victim at a number of stages. For example, California officials have identified five ways in which a

criminal record or other documents may erroneously be created in the name of the victim. The thief may be cited (charged), arrested, prosecuted or convicted in the name of the victim, or the name or identity of the victim may erroneously be associated with a criminal record or other document relating to another individual.[43]

The Scope of the Problem

[69] Precise figures as to the incidence of criminal identity theft are difficult to determine. There is a need for further research on several aspects of criminal identity theft including an understanding of how criminal identity theft occurs, what the short and long-term impacts are, and which groups within the population are affected most adversely.[44] The dearth of research on these and other related issues contrasts with some of the very detailed research now available on these and other issues as they relate to identity theft resulting in financial or other harm not giving rise to a risk of criminal consequences for the victim.[45]

[70] Notwithstanding these difficulties, research confirms the prevalence of criminal identity theft. For example, an examination of data from a National Crime Victimization Survey in 2004 concluded that 4.4% of individuals who identified themselves as victims of identity theft indicated that they had been subjected to a criminal investigation as a result of the misappropriation of their identity.[46] A 2006 study by the United States Federal Trade Commission found that 27% of victims reported that the perpetrator used their name when stopped by law enforcement or when charged with a crime, and 17% of those individuals were the subject of criminal investigation as a result.[47] Methodological and other differences between the studies preclude a direct comparison of these results. Nevertheless, they are a compelling indication of the significance of the problem. Although comparable detailed statistical information is not available from a Canadian perspective, studies have noted that identity theft perpetrated to cover other criminal or terrorist activity is a significant issue.[48]

The Nature of the Harm Caused

[71] This form of identity theft gives rise to both direct and indirect harm. Victims are affected directly when new records or entries in law enforcement records and databases are wrongfully associated or attributed to them. That impact spreads and becomes more difficult to correct as these records or entries are shared with law enforcement or other official organizations

in other jurisdictions. Victims become aware of that impact when they next interact with law enforcement attempting to enforce a warrant or other process generated as a result of that entry, or when they take some step such as renewing a motor vehicle licence or registration. The consequences of that wrongful entry or entries can be severe, including wrongful arrest or detention, or the denial of licensing, registration or other administrative action. Unfortunately, unlike the financial harms associated with identity theft, there is, as yet, no empirical study detailing the scope of this harm, nor of the amount of time it takes to overcome its effects.[49]

[72] Indirect harm may also be caused when official records are used for other purposes, including criminal record checks as a pre-condition to employment, volunteer activity, tenancy, or the production of a driving abstract or similar document in analogous circumstances. Where third parties can access these records, the harm caused can be widespread and insidious. That is especially the case where the data is provided on the basis of a name search only, as opposed to upon the provision of fingerprints or other identifiers. This aspect of the problem may be more acute in the United States, where many official records are commercially available and are used in a wide variety of contexts. The problem is further compounded by the fact that in many of these instances, the searches are "name based" only, and there is no requirement on the third party to disclose that such a search has been conducted.[50]

The Options for Victim Assistance

The United States

[73] The approaches to victim assistance, described in greater detail below, have at least two common characteristics. First, they provide for some mechanism to address the records erroneously created as a result of identity theft. Second, these mechanisms attempt to provide some authoritative method by which the innocent individual can identify themselves as having been a victim of identity theft to law enforcement authorities or others.

Record Correction and Prevention

[74] A national focus group examining this aspect of the issue in the United States described three different approaches that might be taken. The group did not recommend any of these approaches, noting the shortcomings associated with each one. While the group acknowledged the significance of the problem, they concluded that not enough was known about some aspects

of the issue, including the extent to which some of the suggested solutions might adversely affect law enforcement.[51]

[75] These approaches, together with the concerns as articulated by the focus group, are summarized as follows:

a. **Expunging the Identity Theft Related Information** – while some members of the group felt this was the most effective remedy from the victim's standpoint, others pointed out that expunging the information is not appropriate in many instances because even intentionally assumed aliases are valuable pieces of information for law enforcement purposes. Further, if the perpetrator learns that the alias has been deleted, he or she may be able to use it again with impunity. Finally, if the victim's name is the only name on the record, either because the offender has only been arrested once or has used the same alias for multiple arrests, expunging the record may make it difficult or impossible to search the database properly.[52]

   Expunged records may still cause difficulty in background checks as well, as the information may still be included or be confused with the records of first time offenders, which may also be "expunged" in certain jurisdictions.[53]

b. **Sealing the Record(s) in Question** – generally, sealing a record is a less drastic remedy than expunging it. A sealed record would still be available for limited purposes – such as only for criminal justice purposes – but not for other purposes such as background checks.[54]

c. **Flagging the Record(s) in Question** – under this approach, the information would remain available and searchable, but would be flagged or labelled to indicate that it is fraudulent and does not reflect the true identity of the subject, or that it has been the basis of identity theft or mistaken identity. The flag may also indicate that further steps to ascertain the true identity of the individual, such as by fingerprinting. While some members of the focus group felt that this approach would be helpful, a concern was expressed that it may not be fully effective, particularly in settings other than those involving the criminal justice system, because prospective employers or others might not heed the warnings associated with the record, or not confirm by fingerprint

or otherwise that the record in question actually pertains to the subject of the inquiry. Some suggested that the states might enact laws requiring employers or third-party recipients of these records to confirm identity by way of fingerprint in such circumstances.[55]

Victim Identification

[76] Authoritative identification of an individual as a victim of identity theft may assist in minimizing the risk of wrongful arrest, detention or other official action. It may also assist in addressing some of the difficulties that may arise in relation to background or criminal record checks.

Three Approaches to Victim Identification

A. The Identity Theft Registry

[77] California initiated this approach to assist victims of criminal identity theft with the implementation of a registry system for victims in 2001. Several other states have adopted a similar approach.[56] Entry in the California registry is not a simple process. In fact, it requires the completion of eight separate steps.[57]

[78] The most difficult of these involves obtaining a court order which serves as a declaration of factual innocence. The process of petitioning for such an order is complex and requires the filing of a petition, proof of service, preparation of the order, and providing copies of the documentation and support of the application.[58] Information in support of the petition is under a declaration that has the same effect as an oath. Petitioners are advised to avoid including their opinions, conclusions or hearsay.[59] The threshold for granting the application is "that there is no reasonable cause to believe" that the individual committed the offence for which the identity thief was arrested, charged or convicted. If granted, the order compels the sealing and destruction of the records in question.[60] Further, any police reports or records that make reference to sealed arrest reports must indicate that the individual has been exonerated.[61]

[79] Once all of these steps have been completed, the victim is added to the registry, and given a PIN number together with a 24 hour phone number. If stopped by the police, the victim gives

the PIN number together with the phone number to enable the officer to confirm that they have been the victim of identity theft.

[80] Not surprisingly, the complexity of the application process has led to significant difficulties in the implementation of the registry. Testimony before the United States Senate indicated that during the first four years of the registry there were fewer than five registrants. As of March of 2007, that number had only increased to 70.[62]

B. Identity Theft Passport

[81] Ohio initiated a new approach to victim assistance by providing an "identity theft passport". This approach was initiated in December of 2004 in Ohio as a pilot project funded by the federal Department of Justice. The passport identifies the individual as a victim of identity theft and can be used in both criminal and civil contexts. It contains the photograph, fingerprint, signature, and other biometric information of the victim. The passport contains information enabling access to a secure database, available only to law enforcement officers. This database contains other information relating to the identity theft complaint. The information contained in the passport is also forwarded to the motor vehicle database to ensure that additional erroneous entries or other action is not taken based on the identity theft.[63]

[82] According to the National Conference of State Legislatures, six other states have adopted this model – Delaware, Iowa, Maryland, Montana, Tennessee and Virginia.[64] In addition, the President's Identity Theft Task Force recommended that this model, together with a program developed by the FBI, described below, be examined to form the basis of a national program to assist victims of identity theft.[65]

[83] A 2006 report regarding the use of the program in Ohio indicates that it has been widely used. Since 2005 a total of 602 passports have been issued out of 694 applications.[66] Further empirical analysis of the effectiveness of this program is both a condition of the pilot project funding and is contemplated by the identity theft task force described above.

C. The National Crime Information Center Identity Theft File

[84] The FBI maintains a national database accessible by law enforcement agencies. One of the components of this database is the identity theft file. This file was activated in 2005 and

contains approximately 2600 records entered by 29 states. Once a police report has been filed, containing details of the identity theft, together with identifying information pertaining to the victim including a photograph and fingerprints, the report can be entered into the National Crime Information Center (NCIC) identity theft file. The victim selects a password which is included as part of the report. The password is to be confirmed by the police in conjunction with other information to properly identify the victim and ensure that inappropriate enforcement action is not taken in relation to that individual.[67]

The Canadian Context

[85] Both the "passport" and national identity theft file approaches are the subject of continuing evaluation and study in the United States. While this evaluation will provide useful information that should guide policy development in Canada in relation to this issue, there are at least three factors which preclude the wholesale adoption of either approach. They are:

(1) The division of powers and constitutional context.

(2) The restricted use of fingerprinting as a means of identification in Canada.

(3) The more restricted use and disclosure of criminal records in Canada.

[86] The constitutional division of legislative authority adds a significant layer of complexity to any proposal to create a national registry in Canada. As is evident from the review of legislative initiatives undertaken in the United States, many are intended to address both civil and criminal consequences of identity theft. The legislative authority for such a dual purpose registry in the Canadian context is far from clear. Dual or multiple purpose national registries created pursuant to federal legislative authority must address this issue.[68]

[87] Further, any national database would also need to address the issue of information held in provincial databases. While the coordination of statutory authority and data standards and practices might properly be the subject of future work by this conference, other fundamental questions would need to be addressed before that work could be undertaken.

[88] Second, it appears that the collection of fingerprints in identifying and processing arrested persons may be more widespread in jurisdictions in the United States than in Canada. As a result, systems that depend on fingerprint verification for identification could not simply be

imported or adopted in Canada without appropriate consideration of that difference. There are many situations in Canada where no fingerprints are taken as part of the arrest process including summary conviction offences and offences designated pursuant to the *Contraventions Act*.[69] Expanding the categories of offences for which fingerprints may be taken is not a simple solution, particularly where that category may include regulatory matters.

[89] Third, as noted above, it appears that criminal and other court records are freely and commercially available in the United States. As a result, these records are often consulted in a wide range of circumstances, often without the knowledge or consent of the subject of the search. Further, many of these searches are conducted on a "name" basis only, without reference to fingerprints or other information. That is significantly different than the current legislative scheme and practice in Canada.[70] For example, a criminal record check of CPIC requires an application by the subject of the search, a complete set of fingerprints, together with a consent form if the results are to be provided to a third party.[71]

[90] The more restricted availability of these records in Canada, coupled with the differences in search practices may result in a greater incidence of the indirect harm in the United States than in Canada. As a result, any proposals based on the need to address these harms would have to properly account for these differences.

Current Record Practices in Canada

[91] Any attempt to develop an analogous model in Canada must also consider current law enforcement and record repository practices. As a first step in developing an understanding of that context, a brief questionnaire was circulated to all provinces and territories to determine the nature and scope of the databases used to store and access information relating to prior convictions, outstanding warrants, outstanding charges, court orders (release, probation, conditional sentence, DNA etc.), and the extent to which such information is shared between jurisdictions. In addition, they were asked what steps were taken to verify a claim that an entry was the result of identity theft, and what steps were taken once such a claim was verified. The questionnaire also attempted to confirm whether the issue of summary or other convictions not verified by fingerprints was of particular cause of concern in this context. Finally, the questionnaire attempted to determine whether there was a contact group or person in each

jurisdiction responsible for investigating or verifying such claims, and whether a circulation of that contact list across the country would be helpful.

[92] We received eight responses from police agencies, database and court administrators from five jurisdictions. The responses provided some indication of current practices and challenges posed by criminal identity theft. They confirmed that criminal justice information that might be affected by criminal identity theft is stored in a variety of electronic databases and paper archives administered by local and national police agencies, motor vehicle database administrators and court staff. While there are some common features regarding the scope and processes associated with these databases and practices, there are also significant differences.

[93] Common databases in use across the country include:

(1) **Canadian Police Information Centre (CPIC)** – a national computer database maintained by the RCMP, containing a wide range of information including criminal convictions, warrants, alerts, and other information. Criminal record information is verified by fingerprints, but that is not the case with some of the other information.

(2) **Provincial Police or Justice System Databases** – the responding jurisdictions also maintain either province wide police or justice system databases that contain information about outstanding charges, completed cases, release conditions, probation or conditional sentence orders and other restrictions. These systems are based on information either gathered from police services, or court records. While the majority of these systems do not contain outstanding warrants, some do. Much of this information is not confirmed by fingerprint, particularly as it relates to summary conviction, regulatory or provincial offences.

(3) **Provincial Motor Vehicle Databases** – all responding jurisdictions also maintain databases containing registration and related information regarding motor vehicles. These databases also contain records of traffic related convictions and information about license status, and provincial driving suspensions or disqualifications. This information is not confirmed by fingerprints. However,

some jurisdictions use photographs coupled with automated face recognition capabilities to assist in verifying the identity of licence holders.

(4) **Local Police Databases** – many larger municipal and regional police services also maintain databases which also contain occurrence reports and other investigative information.

[94] All jurisdictions share information from these databases between police and prosecution agencies both within and between jurisdictions. Some also make broader use of motor vehicle databases, sharing information from this source with other government agencies for other purposes such as child maintenance enforcement.

Record Correction

[95] All jurisdictions that responded, attempt to correct erroneous records in a variety of ways. All require an investigation to verify the claim of identity theft. In some jurisdictions this is carried out by officers located nearest the complainant, while in others they are investigated by specialized units or groups. Many jurisdictions commented on the complexity of these investigations, and in particular, of the need to balance the appropriate interests of genuine victims of identity theft against those attempting to avoid legitimate obligations or otherwise frustrate the justice system.

[96] Obtaining fingerprints and other unique identifying information from the victim can assist in this process. However, the fact that many of the records in question arise from summary conviction offences, traffic violations, or in other circumstances where fingerprints are not taken is a significant complication in resolving the correct identity of the perpetrator. This is a distinguishing feature between Canadian jurisdictions and many in the United States. Determining what identifying information might appropriately be collected in these circumstances is an issue requiring further study and broad consultation with law enforcement agencies and other interested parties.

[97] Many jurisdictions also expressed an interest in developing a contact list of those individuals or groups involved in these investigations. Such a list would be useful not only in assisting with investigations involving many jurisdictions, but also as an aid in correcting

erroneous information shared with other jurisdictions. It would also facilitate the collection of "best practices" that would assist in streamlining these investigations, and in developing a consistent approach to these issues.

[98] There are also a variety of approaches to the issue of record correction once the investigative stage is completed. These approaches correspond generally with those identified by the focus group described above. Some responding jurisdictions correct the erroneous records generated as a result of identity theft while others retain the original entries with an annotation indicating that the individual identified was a victim of identity theft.

Victim Identification

[99] Responses to the questionnaire revealed three approaches to the issue of victim identification. First, some jurisdictions entered an annotation on CPIC indicating that a record or records were associated with identity theft, and that the named individual was a victim of identity theft. It is not clear whether these annotations contained the detailed information relating to the identity of the victim such as fingerprints, photographs or other descriptors as is the case with the Identity Theft file in the NCIC database described above. Second, some local police agencies provide letters to victims of identity theft that can be produced to law enforcement or others to verify a claim of identity theft. Third, some jurisdictions provide a PIN to a victim of identity theft that can be used by a victim of identity theft to assist in verifying identification and ensuring that erroneous entries are not added to the motor vehicle database, and to assist in the investigation of ongoing identity theft involving the name of that individual.

[100] While there are some broad similarities between some of these initiatives and those undertaken in the United States, it is clear that more study and consultation with law enforcement and other interested parties is required before any recommendation can be made with respect to a particular approach. It is also clear that such a consultation should involve a much broader group of law enforcement personnel, motor vehicle database administrators, and court and registry officials.

Conclusions

[101] While the prevalence and precise nature of the harm caused by criminal identity theft remain to be determined by further research and empirical study, it is clear that this form of identity theft affects a significant number of people and can cause significant harm. While some of the initiatives described in this report show promise in alleviating this harm, all are the subject of further study. It would be premature to recommend the adoption of any of these initiatives in advance of the results of those studies.

[102] Further, significant research is needed to determine the current practices and procedures of law enforcement and other justice system agencies and participants in relation to the creation and correction of records and other information affected by criminal identity theft. A complete and accurate understanding of current practices is needed before the implications of proposed changes can be properly considered.

[103] It is hoped that this aspect of the report may assist in providing some of the foundation for that research. However, the Working Group does not have the composition, capacity or expertise required to carry out that research. Proper consideration of these issues would require a group with representatives from law enforcement, prosecution services, court administrators, motor vehicle registries and others. As a result, the Group recommends that this report be forwarded to Deputy Ministers of Justice for determination of the best forum to consider this important issue.

[104] In addition to the mandate arising from the resolution passed at the last conference, the Working Group also considered what measures might be taken to prevent identity theft, or to enhance the protection of identity information. A first step in identifying how personal information, including identity information, can be misappropriated involved a detailed analysis of that activity. The analysis examines who may improperly obtain information, how it is obtained, how it can be used, and who may be victimized as a result.[72]

[105] With this analysis it is then possible to consider the measures that might be taken to prevent these activities. One approach to such a consideration is reflected in the excerpt from the chart reproduced below. It describes the general nature of the problem of misappropriation of identification or other information, what information is obtained, from whom, and how it is

obtained and used. On the horizontal axis, the chart delineates a series of measures that may address that problem. The measures described fell along a continuum including preventive, administrative, educational, regulatory, statutory, and technical initiatives.

[106] Detailed consideration of both the range of activities that may put identity information at risk together with a broad range of legislative, procedural and educational initiatives taken to offset those risks may provide a valuable foundation for policy development aimed at preventing or limiting the misuse of identity information. In addition, such an analysis may reveal gaps in the response to the misappropriation of identity information in a jurisdiction, or illustrate measures used in another jurisdiction that may be adopted more broadly. Appropriate measures taken to enhance the security of information and strengthen authentication procedures may provide the best protection against identity theft.

[107] Completion of such an analysis on a national basis may be a productive area for further study by the Group. For illustrative purposes, a brief excerpt from this second chart follows:

PROBLÉMATIQUE APPROPRIATION DE L'INFORMATION	SOLUTIONS PRÉVENTIVES	VOLET ADMINISTRATIF	VOLET ÉDUCATIF	VOLET JURIDIQUE LOIS	VOLET JURIDIQUE RÈGLEMENTS	VOLET TECHNIQUE
	Ne pas donner l'information	Catégoriser l'information pour déterminer celle qui peut être exigée d'une personne ou celle dont on peut exiger la consultation Gestion de la consultation et de la diffusion des documents quels qu'en soient les supports. (ne pas limiter cette gestion aux documents circulant sur l'Internet). Exiger l'épuration des documents	Programme de sensibilisation sur le fait qu'il ne faut pas donner de l'information sans que cela soit nécessaire et justifié, en particulier sur la nécessité de la protection des renseignements personnels, des identifiants ou des identificateurs de personnes ou d'objets (cartes)	Législation sur la protection de la vie privée. Interdire la cueillette de renseignements non nécessaires à l'objet de la communication. Déjà fait au Québec, tant dans les secteurs publics que privé. Rendre explicite que cette législation s'applique aussi lorsque l'information est consignée dans	Réglementation sur la diffusion et la destruction de l'information.	Prendre les moyens techniques et opérationnels pour assurer l'habilitation des accès aux documents ou à une partie de l'information qu'ils portent.

		contenus dans les dossiers judiciaires, y compris dans les décisions judiciaires.		un document technologique. Déjà fait au Québec dans la LCJTI.		
	Prévoir l'anonymisation des documents	Faire une directive administrative sur l'anonymisation de l'information, en particulier lors de la cueillette. de l'information dans le cadre, par exemple, d'une recherche ou d'une enquête ou d'un examen. Rendre la directive applicable dans l'ensemble du gouvernement et, par voie contractuelle ou d'ententes, dans les relations avec ses partenaires.	Faire de la formation sur la nécessité et les méthodes d'épuration de l'information contenue dans des documents, particulièrement pour y soustraire les renseignements personnels, avant de rendre ces documents disponibles pour consultation.		Vérifier la possibilité d'appliquer la règle de l'anonymisation dans le secteur privé, en application de la Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., c. P-39.1.)	Prendre avantage des techniques pour masquer certains renseignements et des techniques de chiffrement de l'information.
	Permettre l'utilisation balisée de pseudonymes, de manière à tenir compte du droit des personnes légalement autorisée à obtenir la véritable identité de l'usager du pseudonyme.			Ex: second alinéa de l'article 48, de la LCJTI: «Le nom distinctif d'une personne physique peut être un pseudonyme, mais le certificat doit alors indiquer qu'il s'agit d'un pseudonyme. Les services de certification sont tenus de communiquer le nom de la		

				personne à qui correspond le pseudonyme à toute personne légalement autorisée à obtenir ce renseignement.»		
	Gérer la destruction des documents	Prendre et appliquer une Directive sur la destruction sécuritaire des documents	Publiciser la nécessité de détruire les documents qui ont terminé leur cycle de vie. Par exemple, proposer les techniques de déchiquetage des documents sur support papier.	Appuyer législativement la prise de règles préalables à la destruction de documents et à la protection des renseignements personnels. Ex: l'article 20 de la LCJTI.		
Qui s'approprie l'information?						
Un inconnu	**Empêcher les intrusions par les inconnus**	Mesures opérationnelles: Identification et authentification de l'identité du personnel et des autres personnes ayant droit d'accès aux locaux, à des objets, dont des serveurs, les dossiers ou certains des documents qu'ils comportent. Établir une politique de sécurité de l'information, tant dans les entreprises publiques ou	Faire une campagne de sensibilisation sur l'importance: 1) de déchiqueter les documents papiers que les personnes mettent au rebut, 2) sur les risques des technologies qui permettent l'intrusion, à partir de	Adopter un cadre juridique qui favorise: 1) l'emploi d'une diversité de moyens d'identification et d'authentification d'identité, 2) la mise en place de procédés de certification pour établir un ou plusieurs faits dont l'identification d'une personne, d'un de ses		Mettre en place des mesures de contrôle d'accès à des lieux géographiques, à des immeubles ou à des objets. Adopter des technologies qui ne permettent pas l'intrusion à distance, sans autorisation, dans les objets porteurs de documents technologiques.

		privées, qui tienne autant compte de la sécurité physique, logique qu'opérationnelle et des mesures de gestion documentaire, de manière que des inconnus n'aient pas accès à de l'information qui a de la valeur.	l'externe ou de l'interne, dans les ordinateurs (notamment la technologie sans fil) et sur l'acquisition de technologies qui bloquent les intrusions dans les objets qui servent à la communication.	attributs, droit, pouvoir ou privilège ou l'identification d'un objet ou de leur localisation ou de leur usage. Voir le chapitre III de la LCJTI.		Faire installer des «paravents» sur les guichets automatiques ou des «isoloirs» près des lieux de services où s'effectuent les paiements, afin qu'un inconnu ne voie pas ou n'entende pas l'information associée à la transaction et, en particulier, ne puisse prendre connaissance de l'information permettant le paiement d'un bien ou d'un service.

[108] Unfortunately, the length of this document, 33 pages, precluded its inclusion in this Report. However, this may provide a useful framework for a more detailed consideration of the issues associated with the misuse of identity information, and a useful illustration of the steps that might be taken to minimize the risk of such misuse.

---

[1] That paper is online: http://www.ulcc.ca/en/poam2/Identity_Theft_Paper_En.pdf . The Working Group noted the concerns about the phrase "identity theft", but accepted that the term has become one of convenient usage. Longer term solutions to the issue need a subtler analysis, however, and should not be limited to matters of identity nor to a single focus on questions of theft. One illustration of such an approach is included in the excerpt from the table found in the conclusion to this report.

[2] The full resolution is here: http://www.ulcc.ca/en/poam2/Joint_Civil_and_Criminal_Resolutions_2007.pdf

[3] Whether to legislate on breach notification about personal information that is not otherwise protected by privacy legislation is discussed in section (j) (paragraphs 58 ff.) A province or territory that does not have privacy protection legislation could be asked to pass our uniform law as a free-standing separate obligation. PIPEDA would apply to most but not all such information in such a province.

[4] See for example PIPEDA Schedule 1 s. 4.7 for the principles of safeguards for personal information.

[5] See the site of the Payment Card Industry Security Standards Council: https://www.pcisecuritystandards.org. They require merchants dealing with payment cards to follow certain rules about handing, storage and transmission of credit card information. A quick overview is here: http://en.wikipedia.org/wiki/PCI_DSS. The Canadian Standards Association Model Privacy Code was originally a private standard (or private/public standard), before it became law imposed by PIPEDA. The appendix to Part I of PIPEDA reproduces part but not all of that standard.

[6] See for example the suggestions for encryption standards for mobile devices, as published by the Information and Privacy Commissioner of Ontario in 2007: "Safeguarding Privacy in a Mobile Workplace; Protect the information you keep on your laptops, cellphones and PDAs", http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf.

[7] It might make more sense in this context, therefore, to speak of a "compromise" of security of personal information, rather than of a "breach". The latter term is ambiguous, and could refer to a breach of the applicable standard rather than to a breach of security. Only the latter question is relevant here. However, the literature on the topic tends to use the two terms interchangeably. Whether there has been a "breach" or "compromise" is a different question from whether there has been a sufficient 'loss' to justify notification. That question too is independent – this paper submits – from the degree of compliance with the applicable standard. Reportability is addressed in paragraphs 20 ff.

[8] See for example "A Chronology of Data Breaches" by Privacy Rights Clearinghouse, frequently updated: http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[9] Privacy Commissioner of Canada, "Key Steps for Organizations in Responding to Privacy Breaches", http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp, Step 2, (ii) ("Key Steps"). For similar advice from the United Kingdom's Information Commissioner, see "Notification of Data Security Breaches to the Information Commissioner's Office", http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf.

[10] The Privacy Commissioner of Canada defines privacy breach to include unauthorized collection or use of personal information as well as disclosure. See "Introduction to Key Steps for Organizations in Responding to Privacy Breaches", http://www.privcom.gc.ca/information/guide/2007/gl_070801_01_e.asp. The Information and Privacy Commissioner of Ontario says the same, in "What to do if a Privacy Breach Occurs: Guidelines for Government Organizations", http://www.ipc.on.ca/images/Resources/up-1prbreach.pdf, p. 3 ("What to do"). Nevertheless all the recommendations, and all the statutes on the subject, refer in practice only to unauthorized access to or disclosure of information.

[11] Privacy Commissioner of Canada, "Key Steps", above, note 9, Step 2(iv) and Information and Privacy Commissioners of B.C. and Ontario, "Assessment Tool", below, note 19, Step 1.

[12] K. Kiefer Peretti, "Data Breaches: What the Underground World of 'Carding' Reveals", 25 Santa Clara Computer and High Technology Jl, forthcoming, online:http://www.cybercrime.gov/DataBreachesArticle.pdf.

[13] M. Minik, "Medical ID Theft: A Threat to your Life and Wallet", The National Notary, March 2008, p. 48. There may be more risk of use of medical information where the thief can take advantage of private health insurance already acquired by the person whose information is taken, including running up the maximum benefits under the policy.

[14] See references to case law, note 31. See also a discussion of the availability of insurance for data holders: K.P. Kalinich, "Legal Exposure to the Maxx: Insurance for Breaches of Data Privacy and Information Security", Aon Insurance 2008: http://aon.mediaroom.com/index.php?s=55&item=70 and a blog discussion of this paper on Network World: http://www.networkworld.com/community/?q=node/26203&nlhtsecstrat=rn_032508&nladname=032508securitystrategiesal

[15] There are also costs among data holders. For example, if a merchant compromises the information of holders of credit cards, the card issuer may have to incur the considerable expense of reissuing many cards. In the United States, card issuers have sued merchants to recover these costs, though not yet successfully. D. Rice, "Civil Actions for Privacy Violations 2007: Where are we?" Howard Rice website: http://www.howardrice.com/uploads/content/Civil%20Actions%20For%20Privacy%20Violations%202007%20-%20Where%20Are%20We.pdf at pp 2-4. Some states have enacted legislation to require merchants to compensate card issuers in some circumstances. See Minnesota Statutes ch. 325E, Bill H.F. 1758, http://wdoc.house.leg.state.mn.us/leg/LS85/HF1758.3.pdf. Other states are considering such legislation. T. Probin, Privacy Law Blog, "In response to TJX Privacy breach, one state enacts legislation imposing new security and liability obligations; similar bills pending in five other states", May 29, 2007: http://privacylaw.proskauer.com/2007/05/articles/security-breach-notification-l/in-response-to-tjx-data-breach-one-state-enacts-legislation-imposing-new-security-and-liability-obligations-similar-bills-pending-in-five-other-states .

[16] Privacy Commissioner of Canada, "Key Steps", above, note 9, Step 3.
[17] *Ibid*.
[18] "barring exceptional circumstances." IPC Ontario, "What to do", above, note 10, p.4.
[19] Information and Privacy Commission of British Columbia, "Key Steps in Responding to Privacy Breaches", http://www.oipcbc.org/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf, p. 3. ("Key Steps – BC").
[20] IPC – BC and IPC – ON, "Breach Notification Assessment Tool", December 2006, http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf .
[21] This is essentially what the federal government appears to be proposing for PIPEDA, according to press reports.
[22] This eliminates the "substantial" test for the risk ,but leaves the "serious" test for the harm.
[23] This requires the risk to relate to the statutory standards for treating the information. It does not focus on harm as such, but presumes that the statutory standards were created to prevent harm. This is the recommendation of the CIPPIC submission to Parliament in January 2008. CIPPIC Submission to Industry Canada re: PIPEDA reform issues: http://www.cippic.ca/uploads/CIPPIC_PIPEDAsubm_15Jan08.pdf, page 8ff.
[24] See the discussion below at paragraphs 45 ff about enforcement.
[25] K. Kiefer Peretti, "Data Breaches", above, note 12, at page 28: "These reporting requirements are vital to the ability of law enforcement to investigate the types of crimes involving large scale data breaches". The author is an attorney with the U.S. Department of Justice.
[26] See CIPPIC submission on PIPEDA, above, note 23 page 6.
[27] The term "relevant" privacy commissioner avoids concern with the constitutionality of particular statutes. Quebec has challenged the constitutional status of PIPEDA's privacy rules. The outcome of that challenge may affect which commissioner has the power to act, and thus which will be "relevant" for the present obligation. The resolution of such questions is beyond the scope of this paper.
[28] See above, paragraph 25.
[29] It is beyond the scope of this paper to discuss and a fortiori to provide the other remedies - especially civil – that the law may allow. See however the discussion in paragraphs 53 ff.
[30] Industry Canada's information is at http://strategis.ic.gc.ca/epic/site/oca-bc.nsf/en/h_ca02226e.html.
[31] See for example *Pisciotta* v. *Old National Bankcorp*,(2007) 7th circuit Court of Appeals: http://www.techlawjournal.com/courts/2007/pisciotta_onb/20070823.pdf. American courts, like Canadian, are reluctant to give damages for pure economic loss, which is how they have characterized the harm of identity theft, despite the psychological stress and the time spent making one's reputation good. See A. Ramasastry, "Stolen Laptops and Data Theft", Findlaw.com June 15, 2006: http://writ.news.findlaw.com/ramasastry/20060615.html, However, recently a court refused to strike out a class action based on similar facts:
[32] See the discussion of alternative remedies at paragraphs 53 ff below. A British study of damages awarded for intentional breaches of privacy show that even they are low. Farrer & Co., "Privacy Damages and Harassment", January 2008, http://www.farrer.co.uk/Default.aspx?sID=17&cID=974&ctID=11.
[33] The legislation is reported at Out-law.com on May 12, 2008: http://www.out-law.com/page-9110.
[34] The general U.S. law provides one free check a year. Victims of identity theft are often given additional rights to check for free.
[35] Security freeze legislation in particular is analysed by Consumers Union: http://www.consumersunion.org/campaigns//learn_more/003484indiv.html. See also http://www.financialprivacynow.org and http://www.pirg.org/consumer/credit/statelaws.htm.
[36] A number of private services offer what they say are methods to prevent or repair identity theft. For a review of such services, see http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9083098
[37] There is still a risk that someone will use an existing account, rather than opening a new one.
[38] The ULCC working group has not yet consulted consumer credit reporting agencies about the desirability or management of such a requirement.
[39] For a quick summary as of the end of 2006, see the report of the Privacy Commissioner of Canada to Parliament, Appendix VI: "Overview of American Data Breach Notification Laws": http://www.privcom.gc.ca/parl/2007/sub_070222_06_e.asp. A very thorough "Security Breach Notification Chart" is provided by the Perkins Coie law firm at: http://www.digestiblelaw.com/files/upload/securitybreach.pdf.
[40] It is not clear to the writer whether PIPEDA purports to apply to all personal information in the territories.
[41] 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.
[42] "Report of the BJS/SEARCH National Focus Group on Identity Theft Victimization and Criminal Record Repository Operations", Bureau of Justice Statistics and the National Consortium for Justice Information and Statistics (SEARCH), page 3, available online at http://www.search.org/files/pdf/NatFocusGrpIDTheftVic.pdf.
[43] "How to use the California Identity Theft Registry: A Guide for Victims of 'Criminal' Identity Theft", California Department of Consumer Affairs Office of Privacy Protection, page 2, available online at http://www.oispp.ca.gov/consumer_privacy/consumer/documents/pdf/cis8englsih.pdf.
[44] Presentation of Beth Givens, Director , Privacy Rights Clearinghouse, to the Identity Theft Summit in California, 2005, available online at http://www.privacyrights.org/ar/CASummit-CrimIT.htm, "Establishing a National Research Agenda on Identity Management and Information Protection: Report of the CIMIP Identity Management Research Workshop", pages 16, 28. Center for Identity Management and Information Protection, Utica College July 2007. Research papers from this organization are available online at www.cimip.org.
[45] See for example, "Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement", Gordon, Rebovich, Choo, Gordon, Center for Identity Management and Information Protection, Utica College October 2007.
[46] "First Estimates from the National Crime Victimization Survey: Identity Theft, 2004", Katrina Baum, Bureau of Justice Statistics Bulletin, April 2006.
[47] Federal Trade Commission 2006 Identity Theft Survey Report, at pages 61-4, Synovate, November 2007.
[48] See for example, "Report on Identity Theft", Bi-National Working Group on Cross Border Mass Marketing Fraud, October 2004, available online at http://www.ps-sp.gc.ca/prg/le/bs/report-en.asp#ftn02.
[49] Many reports contain compelling anecdotal accounts. See for example, "Identity Theft" in Problem Oriented Guides for Police: Problem Specific Guide Series No. 25, pages 17-19, Office of Community Oriented Policing Services, United States Department of Justice, Beth Givens presentation, *supra*.
[50] Many articles describe these aspects of the problem, including, Report of the BJS/Search Focus Group, *supra*, at pages 4-5, "Report of the National Task Force on the Commercial Sale of Criminal Justice Record Information", The National Consortium for Justice Information Statistics, 2005, available online at http://www.search.org/files/pdf/RNTFCSCJRI.pdf.
[51] Focus Group, *supra,* at page 8.
[52] Focus Group, *supra,* page 6.
[53] See for example, "Do you have the Background Check Blues" in Privacy Update No.1:8, December 17, 2003, Privacy Rights Clearinghouse. This document is available online at http://www.privacyrights.org/newsletter/031217.htm#3.
[54] Focus Group, *supra,* page 6.
[55] Focus Group, *supra,* page 7.
[56] Minnesota HF 1943, Session 84, Wyoming Senate File SF0053, Arizona HB 2716, Illinois, 20 ICLS 2630/5(b).
[57] How to use the California Identity Theft Registry, *supra*, at pages 2-3.
[58] How to use the California Identity Theft Registry, *supra,* page 5.
[59] How to use the California Identity Theft Registry, *supra,* page 6.
[60] California Penal Code California Penal Code 530.6, 851.8(a)-(d).
[61] California Penal Code 851.8(h).
[62] Testimony of Joanne McNabb, Chief, California Office of Privacy Protection, March 21, 2007, Senate Judiciary Committee. This evidence is available online at http://judiciary.senate.gov/testimony.cfm?id=2582&wit_id=6196. See also, "Locking up the Evil Twin: A Summit on Identity Theft Solutions", March 1, 2005, at page 8. This document is available online at http://www.idtheftsummit.ca.gov/2005_report.pdf.
[63] "Identity Theft Victim Verification/Passport Demonstration Program", Office for Victims of Crime, Department of Justice, February 2004, available online at http://www.ojp.usdoj.gov/ovc/fund/pdftxt/idtheftsolicitation.pdf, "Passport Helps Rescue Ohio Identity Theft Victims", Nevin Barich, National Notary Association, Notary News August 15, 2005, See also http://www.haskinspolice.org/pages/programs/passport-program.php,
[64] "Identity Theft Statutes and Criminal Penalties", June 13, 2006, "2007 Enacted Identity Theft Legislation" National Conference of State Legislatures, available online at http://www.ncsl.org/programs/lis/privacy/idt-legis.htm.
[65] "Combating Identity Theft: A Strategic Plan", April 2007, President's Task Force on Identity Theft, available online at http://www.idtheft.gov/reports/StrategicPlan.pdf.

[66] "Identity Theft Verification PASSPORT Program: Fiscal Year 2006 Annual Report", Crime Victim Services Section, Office of the Ohio Attorney General, available online at http://www.ag.state.oh.us/victim/pubs/06passport_report.pdf.
[67] "The National Crime Information Center Identity Theft File" Vernon M. Keenan, Director, and Marsha O'Neal, Criminal Justice Information System Operations Manager, Georgia Bureau of Investigation, Decatur, Georgia available at http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1186&issue_id=52007. See also, Focus Group, *supra* at page 8, "National Crime Information Center (NCIC) Technical and Operational Update", 06-1, April 28, 2006, available online at http://judiciary.senate.gov/testimony.cfm?id=2582&wit_id=6196. This information can only be included with the consent of the victim, "National Crime Information Center (NCIC) Technical and Operational Update, 06-1, April 28, 2006", available online at http://judiciary.senate.gov/testimony.cfm?id=2582&wit_id=6196, "Information Bulletin 05-14BCIA", National Crime Information Center (NCIC) Identity Theft File, California Department of Justice, June 1, 2005.
[67] For example, constitutional issues related to the subject matter in question were a factor to be addressed in consultations relating to the creation of a DNA Missing Persons Index, available online at http://ww2.ps-sp.gc.ca/publications/Policing/mpi/index_e.asp#7.
[68] For example, constitutional issues related to the subject matter in question were a factor to be addressed in consultations relating to the creation of a DNA Missing Persons Index, available online at http://ww2.ps-sp.gc.ca/publications/Policing/mpi/index_e.asp#7.
[69] Identification of Criminals Act, R.S.C. 1985, C. I-1, s. 2(1).
[70] Personal Information Protection and Electronic Documents Act 2000 c.5, Schedule 1, Principle 4.3. The exemption for designated investigative bodies does not apply in the context of background checks.
[71] For example, see the Instructions for the Civil Fingerprinting Service of the RCMP at http://www.rcmp-grc.gc.ca/crimrec/finger2_e.htm.
[72] Both of the documents described in these paragraphs were prepared by Jeanne Proulx, Counsel and Legislative Draftsperson, Quebec. They are entitled Protection contre l'appropriation d'information, volet prevention, and Appropriation d'information, grille d'analyse. Unfortunately, due to the size of these documents they could not be included in this report, but may be made available on request.