(Ref #CCM: 08002810)

Royal Canadian Mounted Police
Commissioner

Gendarmerie royale du Canada
Commissaire

Guided by Integrity, Honesty, Professionalism, Compassion, Respect and Accountability

Les valeurs de la GRC reposent sur l'intégrité, l'honnêteté,
le professionnalisme, la compassion, le respect et la responsabilisation

JUL 2 2008

Mr. Paul Szabo, M.P.
Chair, Standing Committee on
Access to Information, Privacy and Ethics
c/o Mr. Richard Rumas, Clerk
131 Queen Street, Sixth Floor
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Szabo:

On May 13, 2008, Chief Superintendent Bob Paulson, Acting Assistant Commissioner of the Royal Canadian Mounted Police (RCMP) National Security Criminal Investigations, appeared before your Committee in relation to your study on Privacy Act reform. As requested, I am writing to provide comments to recommendations submitted to the Committee by the Office of the Privacy Commissioner.

Following Chief Superintendent Paulson's appearance, the RCMP undertook a preliminary internal review of the potential impact of the Office of the Privacy Commissioner's recommendations. In this regard, enclosed, for your information, is a document, in both official languages, which highlights issues and concerns raised by the RCMP.

As you know, the RCMP, as the federal police force of Canada, has a presence in every province and territory, and has law enforcement responsibilities in municipal, provincial, federal and international arenas. The real and significant threats from terrorism and organized crime (both domestic and transnational) necessitate that the police have greater flexibility than many other government institutions may require to carry out operations.

.../2

1200 Vanier Parkway
Ottawa, Ontario
K1A 0R2

1200, promenade Vanier
Ottawa (Ontario)
K1A 0R2

This flexibility is, however, accompanied by accountability. Let me assure you that the RCMP is held accountable for its practices through criminal and civil trials, audits by the Office of the Privacy Commissioner and Office of the Auditor General, and through reviews of the Commission of Public Complaints Against the RCMP. In addition, the Government is currently working on the development of additional oversight and review of the RCMP's national security activities.

While the RCMP believes in the underlying strength of the existing legislative framework in balancing individual rights with the collective rights of society, it also recognizes that legislation can always be improved. However, some of the changes to the *Privacy Act* that the Office of the Privacy Commissioner has proposed - depending on how they are implemented - could have a significant negative impact on law enforcement operations, and as a consequence, on the safety and security of Canadians.

I thank the Committee for having consulted with the RCMP on this matter, and trust that the enclosed information will be satisfactory. However, should the Committee require any additional information, we would be pleased to provide it to you.

A version of this letter in the French language is enclosed.

Yours sincerely,

William Sweeney

for William J.S. Elliott

Enclosures

Monsieur Paul Szabo, député
Président du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique
a/s de Monsieur Richard Rumas, greffier
131, rue Queen, 6e étage
Chambre des communes
Ottawa (Ontario)
K1A 0A6

Monsieur,

Le 13 mai 2008, le Surintendant Principal Bob Paulson, Commissaire adjoint par intérim de la Gendarmerie Royale du Canada, s'est présenté devant votre comité pour parler de votre étude sur la réforme de la Loi sur la protection des renseignements personnels (LPRP). Comme vous l'avez demandé à la GRC, je vous écris pour vous transmettre des commentaires sur les recommandations qu'avait soumises à votre comité le Commissariat à la protection de la vie privée.

Suite à la présentation du Surintendant Principal Paulson, la GRC a entrepris à l'interne une étude préliminaire des conséquences possibles de ces recommandations. À cet égard, veuillez trouver le document ci-joint, dans les deux langues officielles, qui expose les questions et préoccupations soulevées par cette étude.

Comme vous le savez, la GRC, en tant que police fédérale du Canada, est présente dans toutes les provinces et dans tous les territoires, et a des responsabilités à tous les niveaux : municipal, provincial, fédéral et international. Le terrorisme et le crime organisé (canadien ou transnational) constituent des menaces réelles et non négligeables faisant en sorte que la police nécessite une plus grande marge de manœuvre que beaucoup d'autres institutions gouvernementales.

.../2

Cette marge de manœuvre doit toutefois s'accompagner d'une obligation de rendre des comptes. Laissez moi vous assurez que la GRC est tenue responsable de ses pratiques, soit lors de procès au criminel et au civil, de vérifications par le Commissariat à la protection de la vie privée et le Bureau du vérificateur général, et d'études par la Commission des plaintes du public contre la GRC. De plus, le gouvernement élabore présentement de nouvelles mesures pour surveiller et évaluer les activités de la GRC qui touchent la sécurité nationale.

Alors que la GRC croit que le cadre législatif existant réussit très bien à équilibrer les droits de l'individu et ceux de la société, elle reconnaît qu'il y a toujours moyen d'améliorer les lois. Cependant, certains des changements à la LPRP qui ont été proposés – selon la façon dont ils seraient mis en œuvre – pourraient compromettre sérieusement l'exécution de la loi et, par le fait même, la sécurité de la population canadienne.

Je remercie le comité d'avoir consulté la GRC sur cette question et espère que le document ci joint sera satisfaisant. Si jamais le comité a besoin de renseignements supplémentaires, nous serons heureux de les lui fournir.

Je vous prie d'agréer, Monsieur, l'assurance de mes meilleurs sentiments.

William J.S. Elliott

pièces jointes

# RCMP Commentary on the Privacy Commissioner's Ten Recommendations for the Reform of the Privacy Act

*(Note: these are preliminary comments based on preliminary consultations)*

***Recommendation Number 1**: Create a legislative "necessity test" which would require government institutions to demonstrate the need for the personal information they collect.*

- Pursuant to its law enforcement mandate, the RCMP has an investigative need to collect personal information and requires some flexibility in the type of personal information collected (i.e., the 'necessity' of some information collected only becomes apparent as an investigation continues).

- More details concerning the proposed legislative 'necessity test' and whether certain law enforcement activities would be exempted would be required to determine how certain activities could be impacted. For example:

    - Depending on the nature of the legislative 'necessity test', there could be adverse implications for the collection of criminal intelligence (especially in the absence of evidence of a specific criminal offence)[1], and on the RCMP's ability to conduct open source searches of publicly accessible web sites while conducting intelligence probes and investigations.

    - If a legislative 'necessity test' increases the threshold on the type of personal data the RCMP are allowed to collect, it would have a negative impact on the ability of the Violent Crime Linkage Analysis System (ViCLAS) and ViCLAS Specialists to identify linkages between cases. Failure to identify linkages would equal a failure to identify violent serial offenders. In a worst case scenario, a serial killer, such as Paul Bernardo, might continue to rape and murder innocent victims because this change prevented or inhibited the RCMP from collecting (and then sharing internally or with other police agencies) the data required to identify the necessary links that would lead to an arrest.

    - In the Privacy Commissioner's February 2008 Special Report on the Examination of RCMP Exempt Data Banks, an example was cited of a neighbour who observed two males carrying something that resembled a large drum, wrapped in canvas, into their house. The concerned citizen

[1] e.g., Information about suspicious behaviour and activity with a possible nexus to national security, which may be indicators of terrorist pre-incident planning or other serious criminal activity (but which may not at first appear to be a criminal offense). Failing to identify and share information about terrorist pre-incident planning activity could prevent the Government from stopping a terrorist incident before it occurs.

called police, who checked it out, but found nothing suspicious. Would the 'necessity test' clearly permit the RCMP to maintain a record of such a 'tip'? What if the true value of the tip only became apparent as an unrelated terrorism investigation continued?

- There could also be potential impacts on the RCMP's ability to engage in open source collection of information on individuals as part of an analysis of national or international trends in crime, or in relation to emerging pressures on existing police programs and planned future initiatives.

- However, if the proposed 'necessity test' follows other models which require that one of three conditions be met (the collection is expressly authorized by statute; the information is collected for the purpose of law enforcement[2]; or the information relates directly to and is necessary for an operating program or activity) then the change might not adversely affect RCMP programs and activities.

[2] Such a 'purpose of law enforcement' condition would need to fully recognize both the breadth and complexity of the personal information collection activities required by the RCMP in order to effectively discharge its mandate.

***Recommendation Number 2**: Broaden the grounds for which an application for Court review under section 41 of the Privacy Act may be made to include the full array of privacy rights and protections under the Privacy Act and give the Federal Court the power to award damages against offending institutions.*

- There needs to be clarification on what array of privacy rights and protections are involved given this could potentially mean a right to damages in many different 'fact situations' involving the collection, accuracy, retention, disposal, use and disclosure of personal information, in the course of the every day management of the RCMP's business – and thus may create 'a chill' in investigative work being carried out as a whole new wave of litigation involving the police could be triggered. Responding to numerous legal challenges would also divert already limited resources away from new and ongoing criminal investigations.

- In making any changes to the *Privacy* Act, there is a need to preserve the integrity and effectiveness of public safety efforts in Canada, and to recognize that privacy is not an absolute right - it is a right that must be delicately balanced against other important societal interests such as the safety and security of Canadians.

- There are already a number of existing checks and balances in place which provide for a system of review of RCMP activities in this area (e.g., criminal and civil trials, reviews by the Commission of Public Complaints Against the RCMP), which should be taken into consideration before any such changes are made to the *Privacy Act*.

- Amongst the issues that would need to be considered regarding this recommendation are:

    - Would this new legal right apply to personal information that was properly subject to an exemption from access under the Act?

    - Given authority already exists in the civil courts to award damages concerning misuse of information held by the police, will such a change introduce an element of duplication and/or redundancy? Is the change even necessary?

    - Would this provision be drafted to have retroactive effect in its application to personal information acquired or used before the proposed new legislative provision was passed into law?

    - Would this proposal permit any individual to exercise this right independently of the role of the Privacy Commissioner – or would the individual first have to complain to the Privacy Commissioner, and have the matter investigated, prior to taking any action in Court?

***Recommendation Number 3**: Enshrine a requirement for heads of government institutions subject to the Privacy Act to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.*

- Privacy Impact Assessments (PIAs) currently involve far more than just the preparation of a document for the Office of the Privacy Commissioner. They also typically involve what can be quite lengthy periods of back and forth consultation concerning the content of the document[3]. Should a legislative requirement for PIAs to be completed prior to implementation be enshrined in the *Privacy Act*, the RCMP may require a special exemption, given some operational matters create a pressing need to implement programs or systems in a time-critical manner (e.g., police response to emergency operations or urgent matters of national security).

    - Such an exemption could potentially take the form of a 'Notification of Intent' to the Office of the Privacy Commissioner, advising of the implementation of a program or system in advance of a PIA. This notification would also serve as a commitment by the RCMP to meet its legislative obligation without impeding its operational mandate.

- Some form of exemption may also be required to allow for the effective testing of intelligence tools developed by the RCMP. For example, the Child Exploitation Tracking System (CETS) assists law enforcement in coordinating intelligence to locate offenders and victims in Canada, and is used to assist international law enforcement in the investigation of sexual exploitation of children on the Internet. CETS undergoes continuous development to improve its ability to be more effective and efficient - requiring that a PIA be completed before the necessary testing and review by the police community is undertaken would seem to be unreasonable (i.e., feedback to enhance CETS would be reduced, the program would suffer, and children could be put at greater risk of abuse).

- Consideration should also be given to the fact that should there be a legislative requirement for PIAs prior to program or system implementation, the Office of the Privacy Commissioner will need to have the capacity to process the submitted material in a more timely fashion than is currently the case (since the implementation of the current Treasury Board policy on PIAs, there have been backlogs of PIAs to be processed by the Office of the Privacy Commissioner).

    - As noted in the CETS example above, it must further be recognized that a PIA is a 'living document' that will need to be continuously updated. Under current practice, there is a flexibility in which amendments can be made

---

[3] Based on RCMP experience, PIAs can take anywhere from 4 months to over one year to reach completion.

through an executive summary that does not necessitate implementation being delayed. The current backlog could be exacerbated should PIA policy be entrenched in legislation as any update to a PIA would require further reviews and approvals before implementation. This would be especially troubling in projects that are phased and include modular improvements in subsequent releases.

  - Should the backlog continue to grow, an additional problem that this change could cause would be that the lag between inception and implementation of technological solutions could result in the RCMP being continuously 'behind the curve'. That is, the time required to process a solution will see it become almost obsolete in the light of advancing technology, by the time it is place.

- The recommendation to publicly report assessment results should also be considered carefully, given a requirement for such reporting could result in the public release of protected investigational tools, techniques and methodologies. Disclosure of these techniques could in some cases have a serious negative impact on the RCMP's ability to conduct investigations (and have potential implications for police officer safety).

  - It must also be recognized that to acquire a number of such tools/technologies, law enforcement agencies such as the RCMP are often required to enter into third party non-disclosure agreements, all under lawful authority and incorporating privacy safeguards, but which prohibit public disclosure.

***Recommendation Number 4**: Amend the Privacy Act to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.*

- Depending on how it is implemented, what is being proposed may be in conflict with the Office of the Privacy Commissioner's other mandated roles - e.g., its role as a neutral and impartial investigator/auditor and its role as a mediator to try to resolve complaints.

- To illustrate this concern, the Committee may wish to consider the distinction between the proposed 'public education' role, and that of acting as the 'unbiased investigator' or 'mediator' in ongoing complaints involving agencies like the RCMP - given that what is being proposed is the power to "publish a compendium of significant cases...notably in the areas of national security, law enforcement" and make "timely public reports on the state of governmental surveillance activities" outside of the process of the existing reporting channel to Parliament.

- In this regard, see also the concerns expressed in relation to Recommendations 3 and 5 with regard to the publication of sensitive information whose disclosure may be injurious to the public interest, as protected by exemption authority provided for in the *Privacy Act* and the *Access to Information Act* (in particular, with respect to information received in confidence from domestic and foreign agencies).

***Recommendation Number 5**: Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.*

- Any changes to the current regime permitting the Office of the Privacy Commissioner to publish information about the RCMP should be considered carefully given the sensitive nature of some of that information, and the fact that it may have been received in confidence, from either a domestic or foreign agency.
    - For example, the proposed changes may raise concerns with international partners that information they have shared in good faith and under strict caveats may be at greater risk of being published. This could result in strained relationships, or even a decrease of intelligence or information received by the RCMP.
- There is also the question of whether the Office of the Privacy Commissioner should be directly making such matters public (through a media release and/or press conference), or whether, as an Officer of Parliament, the Privacy Commissioner should continue, as the current Act envisages, to report on all such matters in the first instance to Parliament.
    - Note that the current Act, at section 39(1), already provides powers for the Office of the Privacy Commissioner to issue 'Special Reports' to Parliament, where the matter is of such urgency or importance that it should not be deferred until the next Annual Report. The Office of the Privacy Commissioner has recently demonstrated the value of this avenue by using it to report to Parliament on the audit of the RCMP exempt banks.
- Another area of potential concern relates to when, in the process governing the privacy management 'practice' in question, this discretion to make a report is to be exercised. Whether it is a Privacy Impact Assessment, or one of the processes laid out by the current Act – e.g., the audit of exempt banks (section 36), the review of compliance with sections 4 to 8 (section 37), or the investigation of a complaint - the existing principle that the process should follow its course through to completion before any report is made to Parliament (and through Parliament to the public) should continue to apply to any publication by the Office of the Privacy Commissioner of information concerning the RCMP.
- If the above concerns are taken into account, providing the Office of the Privacy Commissioner greater discretion to report to Parliament on the privacy management practices of government institutions could be of value in advancing public understanding of particular privacy issues.

***Recommendation Number 6**: Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.*

- The RCMP supports this change as we recognize that all investigative bodies require flexibility and discretion in order to make the most effective use of their limited resources (subject to the exercise of this discretion being reviewable by some other body or person).

***Recommendation Number 7**: Amend the Privacy Act to align it with the Personal Information Protection and Electronic Documents Act by eliminating the restriction that the Privacy Act applies to recorded information only.*

- The full impact on the RCMP of this proposal is not easy to estimate. It would appear to impact two general areas in policing: forensic identification and surveillance:

    - Where one cannot (yet) identify an individual, then the 'sample' (e.g., human tissue, DNA) or fingerprint is not considered personal information (which, by definition, is information about an identifiable individual). However, once a sample/ fingerprint is successfully 'matched' to an identifiable individual, then it would become 'personal information'. Once identified, if it is relevant to the investigative purpose concerned, it is subject almost always to a report in writing, and where this is the case, the RCMP already treats it as 'personal information'. What is less clear, is how in many cases where this identification leads to the elimination of an individual from the inquiry, this proposal would impact the RCMP's *Privacy Act* obligations with respect to s.6 retention, etc.

    - In the area of surveillance systems and technologies, the issue raised is different. In these, the RCMP writes up reports on those individuals who are suspects or targets, and these are already treated as 'personal information'. However, in a video tape, for example, there may be images of many other persons of no investigative interest to the RCMP, and about whom no record may be made, or kept by the RCMP, in terms of either establishing or recording their identification in writing (they may be neighbours, by-standers, or just innocent passers-by, in a video directed at a target). With this proposed change, would the RCMP have a new implicit duty to identify persons of absolutely no interest to its investigative purpose, because of their incidental presence in a recording of a target?

    - With regards to physical surveillance, one question is whether such a change would create a duty to record or duty to identify those surrounding a 'target' in a crowded public place. If the RCMP were required to record and store all information that currently is only being monitored, retention periods and storage issues would also become a major concern that would need to be addressed (both of these issues would have financial and human resources impact on the RCMP).

***Recommendation Number 8**: Strengthen the annual reporting requirements of government departments and agencies under section 72 of the Privacy Act, by requiring these institutions to report to Parliament on a broader spectrum of privacy related activities.*

- While a laudable objective, the impact of such a recommendation would depend on the 'spectrum' of privacy related activities chosen. A very broad spectrum of reporting responsibilities could create a significant - perhaps unattainable - administrative burden for several RCMP programs and services that would require additional resources to aid in the development and validation of tracking and reporting tools (which could serve to detract from where the need for additional resources is most pressing - the core operational and investigative activities of the RCMP).

- A second issue to note is that Parliament already receives annual reports from the RCMP (and all other departments and agencies) in the form of Reports on Plans and Priorities, and Departmental Performance Reports, which require reporting of "significant changes to the organizational structure, programs, operations, or policies" in general, and this proposal might create a measure of redundancy and/or duplication in what Parliamentarians are called upon to read.

- If placed in statute, all of these types of reporting requirements should be subject to the exclusion for sensitive data, systems, operational techniques, methods and technological applications for police purposes.

- The RCMP already provides responses to all of the Office of Auditor General's recommendations, which are made public through being tabled in Parliament, and are subject to the scrutiny of another Parliamentary Committee. In addition, at the discretion of the Office of the Auditor General, the RCMP provides updates on the progress made in implementing these recommendations – which the Auditor General may table in Parliament if she so chooses.

***Recommendation Number 9**: Introduction of a provision requiring an ongoing five year Parliamentary review of the Privacy Act.*

No comment.

***Recommendation Number 10**: Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.*

- Any changes to the *Privacy Act* must recognize that the transnational nature of many forms of crime (e.g., organized crime, terrorism, Internet-facilitated child sexual exploitation) has created unalterable interdependencies among states. Any state that wishes to sustain a safe and secure environment for its citizens must share information internationally.

- The centrality of information sharing to RCMP operations is illustrated by its magnitude and scope, which includes exchanging information that results in assistance to some 5,000 international investigation cases per year through INTERPOL and the exchange of information on approximately 300 cases through EUROPOL.

- The RCMP must share information with foreign states to maintain Canadian public security and protect Canadian citizens, and, as reflected in current policy, readily acknowledges that such sharing must respect human rights and personal privacy. That is why prior to exchanging information or entering into a new agreement with a foreign government, the RCMP takes that state's human rights record into consideration, and why existing RCMP policy requires that caveats be applied to information exchanged, which prohibits the recipient from using or disclosing the information to a third party in a manner that would jeopardize the integrity of the RCMP or the protection of personal information.

- Given the international exchange of information is based on the principle of reciprocity, care must be taken in any changes to the *Privacy Act* not to erode the confidence and trust that has been built up over the years between the RCMP and its international law enforcement partners – a reputation which is already at risk. Such an erosion may increase risks to public safety as a result of critical pieces of information being unavailable to those police officers who need them in a timely fashion.

- While the maintenance of a memorandum of understanding governing information exchanges is a desirable practice (and one in which the RCMP partakes with many partners), the implication that all information exchanges with foreign partners should be governed by written agreements is neither realistic (as not all of our foreign partners are willing to reduce information sharing agreements to writing) or responsible (as police agencies are regularly subject to situations which require urgent action to protect life or property in unforeseen circumstances). It would be difficult for the Canadian public to forgive the RCMP if we ever got to the point where lack of a written agreement delayed one police officer from

talking to another police officer and resulted in a loss of life, or the sexual abuse of a child, or other serious harm to persons or property.

- The suggestion of limiting the disclosure of personal information to "the purpose of administering or enforcing any law which has a reasonable and direct connection to the original purpose for which the information was obtained" could also be highly problematic:

    - What if the RCMP had legal authority to intercept information for the purpose of a Canadian drug investigation and through this intercept learned of plans for a foreign-based suicide bombing - would this mean the information on the suicide bombing couldn't be shared with police in the country where it was to take place?

    - Alternatively, if a routine criminal records check for employment purposes, involved a foreign agency requesting whether one of their citizens, when resident in Canada, had acquired a criminal record, would this 'purpose' have a "reasonable and direct connection" to the fact that the individual had obtained a conviction for dangerous driving in Canada?

    - Integrated Border Enforcement Teams, made up of both Canadian and American agencies[4], share information and work together daily with other local, state and provincial law enforcement agencies on issues relating to national security, organized crime and other criminality transiting the Canada/US border between Ports of Entry. Given officers on these teams often work (literally) shoulder-to-shoulder with each other, would such a legislative change allow them to maintain the continuous and open lines of communication that are so crucial to their success, or would communications become so bogged down in legal technicalities that the teams would be ineffective in carrying out their public safety mandate?

[4] There are currently five core IBET agencies: the RCMP, Canada Border Service Agency, US Immigration and Customs Enforcement, US Customs Border Protection/Border Patrol and the US Coast Guard.

# Commentaires de la GRC sur les dix recommandations de la commissaire à la protection de la vie privée sur la réforme de la *Loi sur la protection des renseignements personnels*

*(Commentaires préliminaires fondés sur des consultations préliminaires)*

***Recommandation numéro 1** : Instaurer par voie législative un « test de nécessité » pour les institutions gouvernementales qui recueillent des renseignements personnels, afin de les obliger à démontrer la nécessité de recueillir ces renseignements.*

- Conformément à son mandat d'application de la loi, la GRC doit recueillir des renseignements personnels dans le cadre de ses enquêtes et a besoin d'une certaine flexibilité en ce qui a trait au type de renseignements personnels recueillis (c.-à-d., le « test de nécessité » concernant certains renseignements recueillis ne devient évident que lorsqu'une enquête se poursuit).

- Des détails supplémentaires sur le « test de nécessité » législatif proposé et sur l'exemption éventuelle de certaines activités d'application de la loi sont requis pour déterminer les répercussions sur certaines activités. Par exemple :

    - Selon la nature du « test de nécessité » législatif, il pourrait y avoir des répercussions négatives sur la collecte de renseignements criminels (surtout en l'absence d'éléments prouvant une infraction criminelle)[1], et sur la capacité de la GRC de mener des recherches « source ouverte » sur les sites Web accessibles publiquement tout en effectuant des enquêtes et des missions de reconnaissance.

    - Si un « test de nécessité » législatif hausse le seuil du type de renseignements personnels que la GRC est autorisée à recueillir, cela nuirait à la capacité du Système d'analyse des liens entre les crimes de violence (SALVAC) et de ses spécialistes de déterminer les liens entre les cas. L'incapacité de déterminer les liens entraînerait l'incapacité d'identifier les agresseurs en série violents. Dans le pire des scénarios, un tueur en série tel que Paul Bernardo pourrait continuer à violer et à tuer d'innocentes victimes parce que ce changement empêcherait la GRC, du moins partiellement, de recueillir (et de communiquer au sein de l'organisme ou à d'autres organismes policiers) les données requises pour établir les liens nécessaires susceptibles de mener à une arrestation.

[1] P. ex., des renseignements concernant des activités et des comportements suspects liés potentiellement à la sécurité nationale, qui peuvent indiquer la planification d'activités terroristes ou d'autres activités criminelles graves (mais qui à première vue ne sembleraient pas être de nature criminelle). L'absence de détermination et de communication des renseignements concernant les activités de planification d'actes terroristes pourrait empêcher le gouvernement de prévenir les incidents terroristes.

- Le rapport spécial de février 2008, déposé par la commissaire à la protection de la vie privée, sur l'examen des fichiers inconsultables de la GRC donne un exemple dans le cadre duquel un voisin avait vu deux hommes transportant un objet ressemblant à un gros tonneau, enveloppé dans une toile, à l'intérieur de leur maison. Le résident inquiet a téléphoné à la police, qui a fait enquête mais n'a rien trouvé de suspect. Le « test de nécessité » permettrait-il clairement à la GRC de conserver un dossier concernant une telle « information »? Et si la valeur réelle de cette information ne devenait apparente que dans le cadre d'une enquête sur le terrorisme qui n'a aucun rapport avec cette intervention policière?

- Il pourrait y avoir des répercussions sur la capacité de la GRC de mener des collectes de renseignements de source ouverte visant des particuliers dans le cadre d'une analyse des tendances criminelles nationales et internationales, ou en relation avec des pressions naissantes sur les programmes actuels de la police et les initiatives futures prévues.

- Cependant, si le « test de nécessité » proposé est conforme à d'autres modèles qui exigent qu'une des trois conditions soit respectée (la collecte est expressément autorisée par un texte législatif; les renseignements sont recueillis aux fins de l'application de la loi[2]; les renseignements sont directement liés et nécessaires à un programme ou à une activité), le changement ne nuirait peut-être pas aux programmes et activités de la GRC.

[2] Une telle condition « aux fins de l'application de la loi » devrait tenir compte pleinement de l'ampleur et de la complexité des activités de collecte de renseignements privés dont a besoin la GRC pour exécuter efficacement son mandat.

***Recommandation numéro 2*** *: Étendre les motifs de recours aux tribunaux en vertu de l'article 41 de la* Loi sur la protection des renseignements personnels *à toute la gamme des protections et droits relatifs à la vie privée que cette loi garantit et autoriser la Cour fédérale à allouer des dommages-intérêts à la charge des institutions contrevenantes.*

- Il faut clarifier la gamme des protections et droits relatifs à la vie privée puisque cela pourrait entraîner un droit à des dommages-intérêts dans de nombreuses « situations factuelles » qui comprennent la collecte, la vérification de l'exactitude, la conservation, l'élimination, l'utilisation et la divulgation des renseignements personnels, dans le cadre de la gestion quotidienne des activités de la GRC. Cela pourrait « freiner » les enquêtes en raison de la nouvelle série de litiges concernant la police qu'il pourrait y avoir. De plus, les ressources déjà limitées serviraient à réagir aux diverses contestations judiciaires au lieu d'être affectées aux nouvelles enquêtes criminelles ou à celles qui sont en cours.

- Lorsqu'il y a une modification de la *Loi sur la protection des renseignements personnels*, il faut préserver l'intégrité et l'efficacité des efforts en matière de sécurité publique déployés au Canada et reconnaître que la vie privée n'est pas un droit absolu – il s'agit d'un droit qu'il faut équilibrer minutieusement avec d'autres intérêts sociétaux importants tels que la sécurité des Canadiens.

- Il existe déjà des freins et contrepoids pour examiner les activités de la GRC dans ce domaine (p. ex., procès criminels et civils, examens effectués par la Commission des plaintes du public contre la GRC), dont il faudrait tenir compte avant que toute modification de ce genre ne soit apportée à la *Loi sur la protection des renseignements personnels*.

- Parmi les enjeux qu'il faudrait prendre en considération au sujet de la présente recommandation, mentionnons les suivants :

    - Ce nouveau droit découlant de la loi s'appliquerait-il aux renseignements personnels qui étaient inconsultables en vertu de la Loi?

    - Puisque les tribunaux civils sont déjà autorisés à accorder des dommages-intérêts en cas de mauvais usage de l'information que possède la police, un tel changement va-t-il entraîner un élément de chevauchement ou de redondance? Ce changement est-il même nécessaire?

    - Cette disposition serait-elle conçue de façon à avoir un effet rétroactif sur les renseignements personnels acquis ou utilisés avant l'adoption de la nouvelle disposition législative proposée?

- Cette proposition permettrait-elle à un particulier d'exercer ce droit indépendamment du rôle de la commissaire à la protection de la vie privée, ou cette personne devrait-elle d'abord porter plainte à la commissaire à la protection de la vie privée, et demander une enquête, avant d'entreprendre toute mesure auprès d'un tribunal?

***Recommandation numéro 3 :*** *Inscrire dans la loi l'obligation, pour les responsables des institutions gouvernementales assujetties à la* Loi sur la protection des renseignements personnels*, d'effectuer une Évaluation des facteurs relatifs à la vie privée (ÉFVP) avant de mettre en œuvre un programme ou un système et d'en publier les résultats.*

- Aujourd'hui, ÉFVP est loin de signifier simplement la présentation d'un document au Commissariat à la protection de la vie privée. Le plus souvent, la réalisation d'une ÉFVP exige des consultations de tous côtés – et qui peuvent s'étirer sur de très longues périodes – sur le contenu du document[3]. Si l'obligation de réaliser une ÉFVP avant la mise en œuvre était inscrite dans la *Loi sur la protection des renseignements personnels* (LPRP), la GRC aurait sans doute besoin d'une exemption spéciale, car dans certaines situations opérationnelles, elle est forcée de mettre en œuvre des programmes ou des systèmes le plus rapidement possible (interventions policières dans des situations d'urgence, questions urgentes touchant la sécurité nationale, etc.).

    - En vertu de cette exemption, la GRC pourrait, par exemple, envoyer au Commissariat à la protection de la vie privée un « avis d'intention » annonçant la mise en œuvre prochaine d'un programme ou d'un système sans ÉFVP préalable. Par cet avis, la GRC s'engagerait également à respecter les exigences de la loi, mais son mandat opérationnel ne s'en ressentirait pas.

- La GRC aurait aussi besoin d'une quelconque exemption pour pouvoir tester efficacement les outils de renseignement qu'elle crée. Par exemple, le Système d'analyse contre la pornographie juvénile (SAPJ) aide les forces de l'ordre à coordonner leurs renseignements pour trouver les délinquants et leurs victimes au Canada, et il est utilisé pour aider les services de police étrangers à mener des enquêtes sur l'exploitation sexuelle d'enfants par Internet. Pour devenir de plus en plus efficace, le SAPJ fait l'objet d'améliorations constantes. L'obligation de réaliser une ÉFVP avant chaque test et avant l'évaluation de ses résultats par la communauté policière nous paraîtrait déraisonnable : nous recevrions moins de commentaires pour améliorer le système, le programme en souffrirait, et les enfants courraient un plus grand risque d'être exploités sexuellement.

- Autre fait à considérer : si la recommandation 3 est appliquée, le Commissariat devra augmenter considérablement sa capacité de traiter les ÉFVP, car ses délais sont déjà trop longs (depuis la mise en œuvre de la dernière politique du Conseil du Trésor sur les ÉFVP, le Commissariat accumule du retard dans le traitement des ÉFVP).

---

[3] La GRC affirme d'expérience que la réalisation d'une ÉFVP peut prendre de 4 mois à plus d'un an.

- L'exemple du SAPJ ci-dessus montre bien qu'une ÉFVP est un document évolutif, qui nécessite des mises à jour constantes. Actuellement, nous avons une certaine marge de manœuvre : il est possible d'inscrire les modifications dans un résumé, sans retarder la mise en œuvre. L'application de la recommandation 3 risquerait d'aggraver le retard accumulé par le commissariat, car tout élément de programme ou de système nécessitant la modification d'une ÉFVP devrait faire l'objet d'encore plus de vérifications et d'approbations avant sa mise en œuvre. Ce problème toucherait encore plus gravement les projets de type progressif, qui requièrent régulièrement des améliorations modulaires.

- Si le problème des retards continuait de s'aggraver, il y aurait un tel délai entre la conception et l'implantation de ses solutions technologiques que la GRC aurait constamment « un siècle de retard ». Vu la rapidité des avancées technologiques, les solutions, au moment de leur application, seraient déjà dépassées.

- La recommandation de publier les résultats des ÉFVP mérite elle aussi d'être réévaluée en profondeur, car son application pourrait rendre obligatoire la publication de techniques, de méthodes et d'outils d'enquête protégés. La capacité de la GRC de mener des enquêtes s'en trouverait parfois gravement compromise (de même que la sécurité des agents).

    - Dernier fait à considérer : pour élaborer ces outils et ces technologies, un service de police comme la GRC doit souvent conclure des ententes de non-divulgation avec des tiers. Ces ententes sont parfaitement légales et elles contiennent des clauses relatives à la vie privée, mais elles interdisent la publication de certains renseignements.

***Recommandation numéro 4 :*** *Modifier la* Loi sur la protection des renseignements personnels *pour confier au Commissariat un mandat clair en matière de sensibilisation du public.*

- Tout dépend de la façon dont elle sera mise en œuvre, mais cette recommandation pourrait entrer en conflit avec certains éléments du mandat du Commissariat à la protection de la vie privée – p. ex. avec son rôle d'enquêteur et de vérificateur neutre, ou avec son rôle de médiateur chargé de régler des plaintes.

- Pour mieux comprendre ce qui nous inquiète, le comité devrait confronter le rôle proposé de « sensibilisation du public » et celui d'enquêteur neutre ou de médiateur dans le traitement des plaintes contre des organismes comme la GRC – compte tenu du fait que les pouvoirs proposés comprennent celui de « publier un recueil des enquêtes importantes [...] notamment dans les domaines de la sécurité nationale [et] de l'application de la loi » et celui de « publier plus régulièrement des rapports sur les activités de surveillance gouvernementale », indépendamment du processus déjà existant de reddition de comptes au Parlement.

- À cet égard, veuillez lire nos commentaires sur les recommandations 3 et 5. Il y est question des renseignements de nature délicate dont la divulgation pourrait nuire à l'intérêt public, et qui sont désignés comme des exceptions dans la *Loi sur la protection des renseignements personnels* et dans la *Loi sur l'accès à l'information* (ici, nous parlons surtout des renseignements obtenus à titre confidentiel d'autres organismes, canadiens ou étrangers).

***Recommandation numéro 5 :*** *Donner au Commissariat une plus grande souplesse pour faire rapport publiquement sur les pratiques de gestion des renseignements personnels des institutions gouvernementales.*

- Toute modification des pratiques existantes qui permettrait au Commissariat à la protection de la vie privée de publier des renseignements sur la GRC mériterait d'être examinée de près, car une partie de ces renseignements sont de nature délicate ou ont été reçus à titre confidentiel d'un organisme soit canadien, soit étranger.

    - Par exemple, si les changements proposés étaient adoptés, nos partenaires à l'étranger pourraient craindre que soient publiés des renseignements qu'ils nous ont communiqué en toute bonne foi et moyennant certaines restrictions sévères. Nos relations avec eux pourraient devenir tendues, et ils décideraient peut-être même de nous communiquer moins de renseignements à l'avenir.

- Autre question légitime : vaudrait-il mieux que la commissaire à la protection de la vie privée publie directement ce genre de renseignements (par des communiqués ou des conférences de presse) ou que, comme agente du Parlement, elle continue de présenter ses rapports d'abord à celui-ci (ce que prévoit la LPRP actuelle)?

    - Il est à noter que le paragraphe 39(1) de la LPRP actuelle autorise déjà le Commissariat à la protection de la vie privée à présenter des « rapports spéciaux » sur les questions dont l'urgence ou l'importance sont telles, selon lui, qu'il serait contre-indiqué d'en différer le compte rendu jusqu'à l'époque du rapport annuel suivant. Le Commissariat a récemment prouvé la valeur de ce paragraphe en présentant au Parlement un rapport sur l'examen des fichiers inconsultables de la GRC.

- Une « pratique » de gestion des renseignements personnels est toujours régie par un processus. La question du stade de ce processus où le commissariat choisira d'exercer son pouvoir de faire rapport publiquement constitue un autre objet de préoccupation. Il existe actuellement un principe voulant qu'aucun rapport ne soit présenté au Parlement (ni au public par le Parlement) avant la fin du processus; ce principe doit continuer de s'appliquer à toutes les publications du commissariat sur la GRC, qu'il s'agisse d'ÉFVP ou de l'un des processus décrits dans la LPRP actuelle, p. ex. les enquêtes sur les fichiers inconsultables (article 36), le contrôle d'application des articles 4 à 8 (article 37) ou le traitement des plaintes.

- Si les inquiétudes susmentionnées sont prises en considération, l'application de la recommandation 5 pourra aider le public à mieux comprendre certaines questions de protection des renseignements personnels.

***Recommandation numéro 6 :*** *Conférer à la commissaire à la protection de la vie privée le pouvoir discrétionnaire de refuser ou d'abandonner une plainte dans les cas où une enquête ne serait guère utile et ne servirait aucunement l'intérêt public.*

- La GRC appuie cette recommandation, car elle croit que tout organisme d'enquête a besoin d'un certain pouvoir discrétionnaire et d'une certaine marge de manœuvre pour pouvoir utiliser d'une manière optimale ses ressources limitées (à condition que l'exercice de ce pouvoir soit examiné par une personne ou un organisme extérieur).

***Recommandation numéro 7*** *: Amender la* Loi sur la protection des renseignements personnels *pour la faire concorder avec la* Loi sur la protection des renseignements personnels et les documents électroniques *en éliminant la restriction selon laquelle la* Loi sur la protection des renseignements personnels *ne s'applique qu'aux renseignements consignés.*

- Il est difficile de déterminer l'effet total de cette proposition sur la GRC. Elle semble avoir des répercussions sur deux secteurs généraux des services de police : l'identité judiciaire et la surveillance :

    - Quand il est impossible (pour le moment) d'identifier une personne, les empreintes digitales ou les « échantillons » (p. ex. tissus humains, ADN) ne sont alors pas considérés comme des renseignements personnels (c'est-à-dire de l'information concernant une personne identifiable). Cependant, lorsque des empreintes digitales ou des échantillons sont « associés » à une personne identifiable, ils deviennent alors des « renseignements personnels ». Une fois identifiés, ils deviennent pertinents dans le cadre de l'enquête concernée et ils font presque toujours l'objet d'un rapport écrit, et lorsque c'est le cas, la GRC les traitent toujours comme des « renseignements personnels ». Il est toutefois plus difficile de déterminer dans combien de cas, où cette identification fait qu'un particulier n'est plus visé par l'enquête, cette proposition influerait sur les obligations de la GRC en vertu de la *Loi sur la protection des renseignements personnels* en ce qui a trait à la conservation mentionnée à l'article 6, etc.

    - En ce qui concerne les technologies et les systèmes de surveillance, l'enjeu soulevé est différent. Dans de tels cas, la GRC rédige des rapports sur les personnes suspectes ou ciblées, et ces dossiers dont déjà traités comme des « renseignements personnels ». Cependant, sur une bande vidéo, par exemple, il peut y avoir des images de bien d'autres personnes non visées par une enquête de la GRC et à propos desquelles la GRC ne peut pas établir ou conserver un dossier, pour ce qui est de déterminer ou de consigner leur identification par écrit (il s'agit peut-être de voisins, de personnes qui étaient dans les environs ou simplement de passants innocents dans une vidéo ciblant une personne en particulier). Avec le changement proposé, la GRC aurait-elle le nouveau devoir implicite d'identifier les personnes qui ne sont d'aucune façon visées par une enquête, et ce, en raison de leur présence fortuite dans un enregistrement ciblant une personne en particulier?

    - En ce qui concerne la surveillance physique, il convient de déterminer si un tel changement entraînerait l'obligation de consigner la présence de personnes entourant une « cible » dans un lieu public achalandé ou de les identifier. Si la GRC devait consigner et stocker tous les renseignements

concernant les activités qui ne sont que surveillées à l'heure actuelle, les périodes de conservation et le stockage deviendraient des enjeux problématiques qui devraient être réglés (ces deux enjeux auraient des répercussions en matière de finances et de ressources humaines sur la GRC).

***Recommandation numéro 8 :*** *Renforcer les exigences touchant les rapports annuels des ministères et organismes gouvernementaux énoncées à l'article 72 de la* Loi sur la protection des renseignements personnels *en obligeant ces institutions à rendre compte au Parlement d'un plus large éventail de pratiques en matière de protection des renseignements personnels.*

- Cette recommandation a certes un objectif louable, mais son incidence dépendrait en grande partie de « l'éventail » de pratiques choisi. Un éventail très large se traduirait par un fardeau administratif pesant, voire insupportable, pour plusieurs programmes et services de la GRC. Ceux-ci auraient besoin de ressources supplémentaires pour les aider à créer et à valider de nouveaux outils de suivi et de reddition de comptes – et cette situation pourrait détourner les ressources supplémentaires des domaines où les besoins sont les plus pressants, à savoir les enquêtes et autres activités opérationnelles centrales de la GRC.

- Deuxième problème, le Parlement reçoit déjà annuellement des rapports de la GRC (et de tous les autres ministères et organismes), qu'il s'agisse de rapports sur les plans et priorités ou de Rapports ministériels sur le rendement. Dans ces documents, la GRC doit faire mention de toute modification importante de sa structure organisationnelle, de ses programmes, de ses activités ou de ses politiques. La recommandation numéro 8 pourrait entraîner redondance et dédoublement dans ce que les parlementaires ont à lire.

- Si toutes ces exigences en matière de rapports annuels sont inscrites dans la loi, il faudra qu'elles contiennent des exceptions pour les renseignements de nature délicate, pour les systèmes, pour les techniques et méthodes opérationnelles et pour les outils technologiques utilisés par la police.

- La GRC applique déjà les recommandations de la vérificatrice générale, qui sont publiques à compter de leur présentation au Parlement et soumises à la surveillance d'un autre comité parlementaire. De plus, la vérificatrice peut demander à la GRC un rapport d'étape sur la mise en œuvre de ses recommandations – rapport qu'elle pourra, à son gré, présenter au Parlement.

***Recommandation numéro 9*** *: Incorporer une disposition exigeant des examens réguliers de la* Loi sur la protection des renseignements personnels *par le Parlement tous les cinq ans.*

Aucun commentaire.

***Recommandation numéro 10*** *: Renforcer les dispositions concernant la communication de renseignements personnels par le gouvernement canadien aux États étrangers.*

- Tout changement à la *Loi sur la protection des renseignements personnels* doit tenir compte de l'interdépendance entre les États résultant de la nature transnationale d'un grand nombre de crimes (p. ex., crime organisé, terrorisme, exploitation sexuelle d'enfants sur Internet). Tout État qui souhaite assurer un environnement sécuritaire pour ses citoyens doit pouvoir communiquer des renseignements à l'extérieur du pays.

- La portée des échanges d'information montre à quel point ces activités sont essentielles aux opérations de la GRC. En communiquant de l'information, la GRC a facilité quelque 5 000 enquêtes à l'étranger par année par l'entremise d'INTERPOL et quelque 300 autres enquêtes par l'entremise d'EUROPOL.

- La GRC doit communiquer de l'information aux États étrangers afin d'assurer la sécurité publique au Canada et de protéger les citoyens canadiens. Comme l'indique sa politique actuelle, la GRC reconnaît d'emblée qu'elle doit respecter les droits de la personne et le droit à la vie privée lorsqu'elle communique de l'information. C'est pourquoi avant d'échanger de l'information, ou d'accepter une nouvelle entente avec un État étranger, la GRC considère la situation envers les droits de la personne dans cet État et pourquoi la politique de la GRC prévoit des restrictions en ce qui concerne la communication de renseignements à des États étrangers. Il est notamment interdit aux destinataires de divulguer l'information à une tierce partie ou de l'utiliser d'une manière qui porterait atteinte à l'intégrité de la GRC ou à la protection des renseignements personnels.

- Étant donné que l'échange d'information à l'échelle internationale est fondé sur le principe de la réciprocité, il ne faudrait pas que les changements apportés à la *Loi sur la protection des renseignements personnels* ébranlent les liens de confiance établis au fil des ans entre la GRC et ses partenaires internationaux. La réputation de la GRC est déjà exposée. Si la confiance s'érode, les agents pourraient ne pas avoir accès en temps opportun à certains éléments d'information, ce qui augmenterait les risques sur le plan de la sécurité publique.

- Il est souhaitable dans la pratique de conclure des protocoles d'entente sur la communication de renseignements, ce que la GRC a fait avec bon nombre de partenaires. Cependant, il n'est ni réaliste, ni responsable de s'attendre à ce que tous les échanges d'information avec des partenaires étrangers soient régis par des accords écrits, d'abord parce que certains partenaires étrangers ne sont pas prêts à mettre par écrit les règles en matière d'échange d'information, et ensuite parce que les organismes de police font souvent face à des situations imprévues où ils doivent agir rapidement pour sauver des vies ou protéger des biens.

Le public canadien aurait de la difficulté à pardonner la GRC si, en raison de l'absence d'un accord écrit, un agent de police tardait un jour à communiquer de l'information à un autre, et que ce retard occasionnait un décès, un acte de violence sexuelle envers un enfant ou autre préjudice grave à une personne ou à des biens.

- La suggestion voulant « que les renseignements personnels ne peuvent être communiqués qu'à des fins d'administration ou d'exécution d'une loi ayant un lien raisonnable et direct avec la fin pour laquelle les renseignements ont été initialement obtenus » pose aussi d'importants problèmes :

    - Que se passerait-il si la GRC, en exerçant légalement le pouvoir d'intercepter une communication dans le cadre d'une enquête au Canada sur une affaire de drogues, prenait connaissance d'un complot en vue d'un attentat suicide à la bombe dans un autre pays? La GRC pourrait-elle, en vertu d'une telle disposition, communiquer avec les services de police du pays concerné?

    - Par ailleurs, si dans le cadre d'une vérification courante des antécédents criminels aux fins d'emploi, un organisme étranger demande si l'un des citoyens de son pays a eu un casier judiciaire pendant son séjour au Canada, est-ce que cette « fin » a un « lien raisonnable et direct » avec le fait que la personne en question a été condamnée pour conduite dangereuse au Canada?

    - Par ailleurs, les équipes intégrées de la police des frontières, composées de représentants d'organismes canadiens et américains[4], travaillent avec d'autres organismes d'application de la loi locaux, étatiques et provinciaux, et tous les jours échangent avec eux de l'information sur des problèmes liés à la sécurité nationale, au crime organisé et à d'autres activités criminelles menées aux points d'entrée à la frontière canado-américaine. Les membres de ces équipes travaillent souvent côte à côte. Un tel changement à la loi leur permettrait-il de continuer à communiquer ouvertement, ce qui est essentiel à leur réussite, ou la communication sera-t-elle entravée par des formalités judiciaires qui empêcheraient les équipes de s'acquitter de leur mandat en matière de sécurité publique?

[4] À l'heure actuelle, cinq grands organismes participent aux EIPF, soit la GRC, l'Agence des services frontaliers du Canada, la US Immigration and Customs Enforcement Agency, la US Customs Border Protection/Border Patrol Agency et la garde côtière américaine.