Le 8 février 2017

Monsieur Blaine Calkins, député
Président
Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes
Chambre des communes
Ottawa (Ontario)  K1A 0A6

Monsieur le Député,

L'Association nationale de destruction de l'information – Chapitre canadien (NAID-Canada) attend avec impatience la prochaine étude par votre comité de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Le Canada jouit traditionnellement d'une réputation de leader mondial en matière de protection des renseignements personnels, mais cette image a commencé à se détériorer au cours des dernières années, après que d'autres pays ont adopté des mesures plus strictes en la matière.

En fait, maintenant que le nouveau *Règlement général sur la protection des données* (RGPD) de l'Union européenne a été adopté, on ne peut manquer de constater l'absence d'une application rigoureuse et d'un renvoi significatif à des mesures de contrôle des fournisseurs de services au Canada, ajouté au fait que la loi canadienne sur la notification des atteintes à la protection des données, pourtant adoptée il y a plus d'un an et demi, n'est toujours pas entrée en vigueur.

En guise de contexte, NAID-Canada est l'association à but non lucratif nationale qui représente les sociétés spécialisées dans les pratiques sûres de destruction des renseignements personnels et des documents. Notre mission consiste à sensibiliser et à mieux faire comprendre l'importance de telles pratiques. Nous voulons ainsi éviter l'utilisation des renseignements confidentiels, personnels et commerciaux à une autre fin que celle à laquelle ceux-ci étaient initialement destinés. NAID-Canada participe aussi activement à l'élaboration et à la mise en œuvre de normes et d'une certification de l'industrie, en plus d'offrir un éventail de services à ses membres, comme des services de représentation, de communication, de formation et de perfectionnement professionnel.

Veuillez trouver ci-joint un ensemble de propositions visant à faire modifier la LPRPDE et ainsi à remédier au problème persistant qu'est l'omission de détruire en toute sécurité des renseignements périmés. Notre principale recommandation consiste à inclure dans la LPRPDE une définition de la destruction de renseignements ainsi qu'une exigence

explicite à l'endroit des organisations d'éliminer de façon sécuritaire les renseignements qui ne sont plus nécessaires.

À l'occasion de son étude de la LPRPDE, en 2007, le Comité a appuyé la recommandation de définir la destruction, sans que cela entraîné de modifications législatives. Depuis ce temps, d'autres pays ont emboîté le pas, permettant ainsi à leurs citoyens de jouir d'une plus grande protection de leur vie privée. De plus, beaucoup d'autorités compétentes, particulièrement au palier des différents États américains, imposent maintenant des amendes considérables aux organisations qui ne détruisent pas les renseignements de façon sécuritaire. Nous estimons donc que le Canada devrait envisager de prendre des mesures similaires. Diverses instances gouvernementales au Canada, comme celle de l'Alberta, ont déjà octroyé à leurs autorités compétentes le pouvoir d'imposer des amendes à cet égard.

La documentation ci-jointe contient de plus amples renseignements sur ces questions. Nous serions heureux de pouvoir témoigner devant votre comité dans le cadre de votre examen.

Finalement, veuillez prendre note que la NAID mène actuellement la plus grande étude scientifique connue à ce jour sur les dispositifs de mémoire d'occasion, dont nous dévoilerons les résultats lors de notre conférence annuelle, qui aura lieu en mars. Plusieurs études antérieures, y compris celle du commissaire à la protection de la vie privée du Canada, ont révélé que les appareils électroniques mis au rebut ou recyclés ne sont pas adéquatement purgés des renseignements personnels qu'ils contiennent. Le communiqué de presse annonçant cette étude est joint à la présente; nous en transmettrons les résultats au Comité dès leur diffusion.

Je vous remercie de votre attention. N'hésitez pas à communiquer avec le soussigné pour toute question à ce sujet.

Veuillez agréer, Monsieur le Député, mes plus cordiales salutations.

K. Backman

Le président,
NAID-Canada,

Kristjan Backman

c. c. Membres du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes
M. Hugues La Rue, greffier du Comité

# Dévoilement prochain de la plus importante étude sur les dispositifs électroniques d'occasion

**Le 25 janvier 2017**

La recherche compte depuis longtemps parmi les outils que la NAID emploie pour éduquer le public et les décideurs. Au cours des années, elle a d'ailleurs joué un rôle dans les campagnes de sensibilisation liées à la réglementation ainsi que dans l'élaboration des normes, rehaussant de ce fait considérablement la crédibilité de l'association. En poursuivant cette tradition, la NAID mène actuellement la plus importante étude scientifique connue à ce jour sur les dispositifs de mémoire d'occasion, dont les résultats seront dévoilés à la prochaine conférence annuelle.

Aux dires du premier dirigeant de la NAID, Bob Johnson, il s'agit du type de recherche qui distingue la NAID de ses pairs. « Les conférences, les revues et les certifications en quête d'appui ne manquent pas, a affirmé Johnson. À ma connaissance, toutefois, la NAID est la seule dont la feuille de route soit aussi riche lorsqu'on parle de réinvestir cet appui économique dans la recherche afin de promouvoir et de faire avancer l'enjeu qu'est la destruction sécuritaire des données. »

C'est un organisme indépendant qui mène cette étude, quoique la NAID l'ait commandée, afin de garantir la fiabilité et l'intégrité des résultats. Les conclusions précises ne pointeront aucune organisation du doigt (les résultats seront regroupés), mais elles seront mises à la disposition des autorités de réglementation dans l'éventualité où celles-ci souhaiteraient les étudier davantage.

Au cours des 20 dernières années, des études ont été effectuées périodiquement sur des disques durs achetés sur le marché des produits d'occasion. La première étude connue s'est déroulée de 2000 à 2003, lorsqu'une équipe dirigée par Simson Garfinkel a fait l'acquisition de 158 disques durs d'occasion provenant de sources aléatoires, puis les a soumis à une analyse par des experts. L'IEEE a publié les résultats de son étude la même année dans sa revue *Security & Privacy*, dans un article intitulé *Remembrance of Data Passed*, lequel rapporte qu'un pourcentage important des disques durs d'occasion choisis au hasard contenaient des renseignements personnels. Si surprenant que soit ce résultat, les chercheurs ont aussi été étonnés de découvrir que certains des disques durs contenant des renseignements personnels avaient précédemment été déployés dans des établissements gouvernementaux, des services financiers ou des établissements de soins de santé, tous assujettis à une réglementation protégeant leurs données. Autre fait inquiétant : beaucoup de disques durs contenant des renseignements personnels montraient des signes qu'on avait tenté de remplacer ces données par d'autres. Cela signifie donc que l'ancien propriétaire du disque croyait en avoir effacé toutes les données, alors que, réellement, il n'en était rien.

L'Institut de recherche du CHEO, qui a son siège au Canada, a effectué une étude similaire en 2007; la NAID a reproduit cette étude en Australie en 2013 et le Blancco Technology Group a lui aussi publié une étude semblable en 2016. Leurs résultats allaient tous dans le même sens. Dans chacune d'elles, des renseignements réglementés ou concurrentiels ont été découverts dans une proportion considérable de disques durs.

L'étude que la NAID vient tout juste de mener en 2017 sur des dispositifs de mémoire d'occasion porte sur 250 unités; elle comprend des disques durs traditionnels ainsi que des disques à circuits intégrés (SSD). La NAID a déjà mené des études sur les pratiques d'élimination au Canada, en Espagne et au Royaume-Uni, ainsi que sur les attitudes des consommateurs aux États-Unis et en Europe.

Nous croyons qu'il est important pour les membres de la NAID de connaître les types d'initiatives sur lesquelles l'association se concentre. Les résultats complets de l'étude actuelle seront dévoilés à l'occasion du congrès de 2017 de la NAID. L'événement comportera d'autres dévoilements, comme celui de la première édition du manuel sur l'élimination des renseignements.

Nous encourageons tous les professionnels de la destruction de renseignements à prendre part à cette initiative inédite.

**Mettre un terme à la violation accidentelle de données**

NAID-Canada croit que la sécurité de l'information est fonction de la protection qui lui est accordée à son point névralgique dans son cycle de vie. Trop souvent, on porte peu d'attention à l'étape finale du cycle de vie d'un document et à la destruction et à l'élimination de ce dernier. Les reportages quasi quotidiens sur la découverte de renseignements personnels dans les bennes à ordures, les conteneurs de recyclage ou les immeubles abandonnés ou sur les ordinateurs et autres appareils électroniques jetés en sont la preuve. Toutes les mesures de protection des renseignements personnels pendant leur vie utile ne servent à rien si la destruction de ces derniers n'est pas définitive.

Comme preuve tangible, NAID-Canada a publié, en octobre 2010, les constatations d'un rapport de vérification ayant porté sur les pratiques en matière de destruction de données dans l'agglomération de Toronto. On a ainsi découvert que 14 % des bennes à ordures dans le secteur commercial de l'agglomération contenaient des renseignements personnels confidentiels, un pourcentage outrageusement élevé. Dans certains secteurs, les chiffres étaient accablants. Soixante-quinze pour cent (75 %) des cabinets de médecin examinés avaient laissé des renseignements personnels dans des bennes à ordures placées sur la voie publique. Quant aux concessionnaires automobiles, tous étaient fautifs.

NAID publiera bientôt une nouvelle étude sur les produits électroniques recyclés.

NAID-Canada plaide depuis longtemps en faveur de l'inclusion d'exigences précises de destruction dans la loi sur la protection de la vie privée, y compris une définition de « destruction ». Le Canada n'a pas ce genre de dispositions, mais il serait facile de les mettre en place en modifiant la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). C'est peut-être le seul moyen d'obliger les organisations à porter à cet aspect souvent oublié de la protection de la vie privée l'attention qu'il mérite.

**Modifications nécessaires à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)**

NAID-Canada recommande les modifications suivantes à la LPRPDE :

- Définir le mot « destruction » comme désignant la « disparition absolue de documents afin de les rendre inutiles et pour que la récupération de l'information, en tout ou en partie, soit impossible ».
- Ajouter une clause stipulant qu'une organisation doit détruire les renseignements personnels dont elle n'a plus besoin.

Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a approuvé l'ajout d'une définition de « destruction » dans la LPRPDE lorsqu'il a examiné cette loi la dernière fois, en 2007. On trouvera plus loin d'autres informations sur la manière de procéder pour y arriver.

***Ajouter une définition de « destruction »***

Actuellement, la LPRPDE ne contient aucune définition de « destruction ». NAID-Canada recommande donc d'ajouter la définition suivante dans la section correspondante du texte législatif :

> « Destruction » signifie l'altération physique des documents de façon à les rendre inutiles et à rendre impossible la récupération de l'information, en tout ou en partie. « Détruire » signifie altérer jusqu'à faire disparaître.

Cette définition s'applique aux documents sur support papier ou électronique. Des variantes ont été intégrées à la loi sur la protection de la vie privée dans plusieurs provinces et territoires du Canada et dans d'autres pays, notamment aux États-Unis.

***Modification de l'article 3 de la LPRPDE***

L'article 3 de la LPRPDE annonce l'objet de la Loi. NAID-Canada recommande d'ajouter les mots soulignés ci-après à cet article :

> *La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation, la communication et la destruction de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.*

Cette modification insiste sur le fait que les organisations doivent inclure les moyens de détruire définitivement les renseignements personnels dans leur politique en matière de protection de la vie privée.

***Modification de l'article 5 de la LPRPDE***

L'article 5 de la LPRPDE devrait être modifié pour y ajouter l'obligation formelle de détruire. Il se lirait comme suit, le paragraphe ajouté étant souligné :

> *5(1) Sous réserve des articles 6 à 9, toute organisation doit se conformer aux obligations énoncées dans l'annexe 1.*
> *(2) L'emploi du conditionnel dans l'annexe 1 indique qu'il s'agit d'une recommandation et non d'une obligation.*
> *(3) L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.*
> *(4) L'organisation doit obligatoirement détruire les renseignements personnels dont elle n'a plus besoin.*

Ce qui nous préoccupe à ce sujet, c'est l'énoncé du paragraphe 4.5.3 de l'annexe 1 de la LPRPDE :

> *On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer*

> *des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.*

Cet énoncé pose deux problèmes. D'abord, l'emploi du conditionnel au paragraphe 4.5.3. Comme le stipule le paragraphe 5(2) cité auparavant, [l]'emploi du conditionnel indique qu'il s'agit d'une recommandation et non d'une obligation. NAID-Canada croit que la destruction définitive des renseignements personnels doit être obligatoire. Elle ne doit pas être laissée à la discrétion des organisations.

Ensuite, les termes « détruire, effacer ou dépersonnaliser » sont trop vagues. Nous en avons déjà discuté avec Innovation, Sciences et Développement économique Canada et ce dernier a convenu que le paragraphe 4.5.3 donne lieu à plusieurs lectures.

Par conséquent, la modification proposée à l'article 5 permettrait de bien faire comprendre aux organisations qu'elles doivent détruire les renseignements personnels dont elles n'ont plus besoin. Elles devront dès lors procéder de manière à se conformer aux critères énoncés dans la définition proposée de « destruction ».

**Retrouver la confiance de la population**

NAID-Canada croit qu'une définition claire du terme « destruction » est essentielle à plus d'un titre et non seulement pour des motifs liés à la protection des droits de la personne. C'est aussi une nécessité d'ordre pratique. La violation des droits d'autrui en mettant négligemment au rebut leurs renseignements personnels nourrit grandement ce qui est devenu un fléau à l'échelle mondiale, soit le vol d'identité et la fraude.

Ainsi, une étude américaine révèle que la grande majorité des vols d'identité est le résultat de la faible technologie employée en lien avec l'accès aux renseignements personnels, par exemple, la fouille des bennes à ordures ou la mise à la poubelle. En effet, les agents chargés de faire respecter la loi aux États-Unis ont mis au jour des bandes du crime organisé qui exploitent avec grand art cette source immédiate de renseignements personnels. Ces bandes répartissaient le travail dans leurs rangs, les plus bas dans l'échelle s'occupant de ramasser l'information dans les poubelles pour la remettre aux échelons supérieurs ayant reçu la formation nécessaire pour l'exploiter au mieux.

Le phénomène a entraîné l'adoption d'une nouvelle famille de législations aux États-Unis, illustrée par la loi sur les opérations de crédit justes et exactes, la *Fair and Accurate Credit Transactions Act (FACTA),* et une foule de lois d'État, qui visent non seulement à protéger la vie privée, mais à endiguer également la vague de vols d'identité et de fraudes. Par conséquent, il existe une différence marquée dans la formulation des modalités réglementaires s'appliquant au retrait des renseignements personnels, et les sanctions en cas de non-conformité.

Alors que l'ancienne réglementation liée au retrait des renseignements personnels obligeait à limiter leur consultation par des personnes non autorisées, les nouveaux règlements exigent que des mesures soient prises pour détruire les renseignements personnels avant que les documents les contenant ne soient éliminés. En outre, la nouvelle famille de législations exige que ces mesures de sécurité soient étayées dans les politiques de l'organisation.

Recommandation : Exiger des organisations qu'une politique de destruction fasse partie de leur politique générale en matière de protection de la vie privée.

Ajoutons à ce sujet qu'un rapport, en janvier 2016, de la commissaire à l'information et à la protection de la vie privée de l'Alberta, à la suite d'allégations de déchiquetage incorrect de documents au sein du ministère de l'Environnement et du Développement durable dans le secteur des ressources, a entraîné la publication de plusieurs recommandations concernant la conservation et la destruction des renseignements personnels. NAID-Canada tient à en citer une en particulier, soit que le gouvernement [traduction] « mette en ligne tous les calendriers des délais de conservation des documents opérationnels afin que la population puisse les consulter, favorisant ainsi la clarté, la cohérence et la reddition de comptes face aux décisions prises quant à la politique de conservation des documents gouvernementaux ».

Il y a des parallèles à établir avec le secteur privé. Par exemple, si cette dernière recommandation devait être adoptée, il serait logique d'exiger des organisations qu'elles affichent leur propre politique de destruction des renseignements personnels. Les organisations seraient d'autant motivées à se conformer et les consommateurs seraient en mesure de déterminer les entreprises qui offrent les meilleures pratiques en matière de protection de la vie privée.

Recommandation : Exiger des organisations qu'elles affichent leur politique en matière de destruction des renseignements personnels.

## Mesures d'application et conformité

La loi en matière de protection de la vie privée n'est efficace que dans la mesure où les organisations s'y conforment. Il faut du coup s'assurer que les employés comprennent et respectent la loi. NAID-Canada a constaté que le simple fait d'avoir une politique n'entraîne pas nécessairement le respect de celle-ci, lorsque le personnel d'une organisation ne sait pas qu'elle existe ou ne la respecte pas.

La solution à ce problème, c'est la sensibilisation, la formation appropriée et continue et, au besoin, des sanctions en cas de violation de la loi. Plusieurs pays vont dans cette direction, certaines atteintes à la vie privée méritant à leurs yeux la prise de sanctions.

Par exemple, un groupe médical du Massachusetts a été condamné à une amende de 140 000 $US pour avoir jeté 67 000 dossiers médicaux dans une décharge sans avoir clavardé ou déchiqueté les documents au préalable[1]. Dans une autre affaire, le département américain de la Santé et des Services sociaux a convenu d'une amende de 800 000 $US avec une société de l'Ohio qui avait laissé 5 000 à 8 000 dossiers médicaux dans l'allée de garage d'un médecin[2]. Encore une fois aux États-Unis, la Federal Trade Commission (FTC), ou commission fédérale du commerce, a condamné un agent immobilier de Las Vegas à une amende de 35 000 $US pour avoir abandonné 40 boîtes de documents financiers (déclaration de revenus, relevés bancaires, rapports de

[1] Voir https://nakedsecurity.sophos.com/2013/01/15/medical-patients-health-records-dump/.
[2] Voir http://www.hhs.gov/about/news/2014/06/23/800000-hipaa-settlement-in-medical-records-dumping-case.html#.

solvabilité, etc.) dans une simple benne à ordures[3]. Pendant ce temps, un groupe médical du Missouri risquait une amende pouvant atteindre 1,5 million de dollars pour avoir abandonné des dossiers médicaux dans une simple benne à ordures[4].

Pour ce qui est de la destruction de renseignements personnels, rien ne saurait excuser l'omission de le faire de manière sécuritaire et sûre. Comme le montrent les décisions judiciaires susmentionnées, les administrations fédérale et des États prennent cette question très au sérieux et condamnent à de lourdes amendes.

Recommandation : Autoriser le commissaire à la protection de la vie privée à condamner à une amende toute personne qui porte atteinte à la vie privée de manière flagrante ou systématique.

**Perte du rôle de meneur par le Canada**

Le Canada n'est plus considéré comme un leader mondial en matière de protection de la vie privée. Il a perdu sa réputation alors que d'autres pays adoptaient des mesures de protection de la vie privée plus strictes. Dans notre propre secteur de la protection de l'information, nous avons étayé ci-haut la nécessité d'une plus grande clarté de la part des gouvernements quant à ce qui constitue une destruction et aux lourdes amendes encourues pour avoir omis de détruire définitivement des renseignements qui ne sont plus utiles.

NAID-Canada croit que les modifications proposées redonneront au Canada sa réputation de leader et, surtout, assureront aux Canadiens la protection accrue de leurs renseignements personnels dont jouissent les habitants d'autres pays.

[3] Voir http://www.lexology.com/library/detail.aspx?g=5af8a709-0850-487d-bc74-4db192e80ff1.
[4] Voir http://www.hipaajournal.com/hipaa-settlement-reached-dumpster-phi-exposure/.