29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Atelier
Tueur de dragons
L'évaluation des facteurs relatifs à la vie privée
Les problèmes et les méthodes pour les autorités de réglementation

Workshop
Dragon Slayer
Privacy Impact Assessment
Issues and Approaches for Regulators

27 septembre/September 27
13h30 – 16h

Série Terra Incognita, cahier de travail # 12/Terra Incognita, workbook series # 12

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Table des matières / Table of contents

Biographies

M. Blair Stewart — Président 2

M. Claude Beaulé 2

M. LeRoy Brower 3

M. David Flaherty, Ph. D. 3

M. Donald Lemieux 4

M^me^ Rebecca Richards 5

M. Trevor Shaw 5

M. Mark Vale 6

M. Nigel Waters 7

Évaluation des facteurs relatifs à la vie privée : enjeux et approches pour les organismes de réglementation 9

Les évaluations des facteurs relatifs à la vie privée : de la théorie à la pratique 20

Critères permettant d'établir la pertinence des évaluations des facteurs relatifs à la vie privée (ÉFVP) au Canada 27

Modèle pour les évaluations des facteurs relatifs à la vie privée 40

Biographies

Mr. Blair Stewart — Chair 2

Mr. Claude Beaulé 2

Mr. LeRoy Brower 3

Dr. David Flaherty 3

Mr. Donald Lemieux 4

Ms. Rebecca Richards 5

Mr. Trevor Shaw 5

Mr. Mark Vale 6

Mr. Nigel Waters 7

Privacy Impact Assessment: Issues and Approaches for Regulators 9

Getting Through Privacy Impact Assessments 20

Criteria for Evaluating the Adequacy of Privacy Impact Assessments (PIAs) in Canada 27

Privacy Impact Assessments Template . . . 50

Biographies

Président : M. Blair Stewart

Blair Stewart est commissaire adjoint à la protection de la vie privée en Nouvelle-Zélande. M. Stewart travaillait dans un cabinet de droit commercial à Auckland avant d'entrer au Commissariat à la protection de la vie privée, dès sa création en 1993. Il s'occupe de la politique sur la protection de la vie privée, des codes de pratique, de la technologie et des questions internationales. Il a collaboré au travail de protection de la vie privée à l'échelle internationale par le biais du Asia Pacific Privacy Authorities Forum et à titre de membre du sous-groupe sur la protection de la vie privée de l'APEC ECSG, depuis sa mise en place. Il a mis l'accent sur l'élaboration de mécanismes institutionnels et de réglementation à la fois efficaces et souples visant à protéger les renseignements personnels à l'échelle nationale et supranationale. Depuis 1996, Blair préconise l'évaluation des facteurs relatifs à la vie privée en tant qu'outil simple pour les décideurs et les responsables de la réglementation qui doivent faire face aux défis à la fois complexes et nouveaux que présente la technologie sur le plan de la protection de la vie privée. En 2002, Blair a publié *Privacy Impact Assessment Handbook*, ouvrage qui a eu une influence tant en Nouvelle-Zélande qu'à l'étranger. Il est titulaire d'un baccalauréat ès arts et d'un baccalauréat en droit de l'Université d'Auckland et il a été reçu avocat à la Haute Cour de Nouvelle-Zélande et à la Cour Suprême de l'Angleterre et du pays de Galles.

Conférenciers

M. Claude Beaulé

Claude Beaulé est consultant en matière de vie privée. Il a commencé sa carrière dans le domaine de la protection de la vie privée en 1978 aux Archives nationales du Canada. Il y a d'abord répondu aux demandes de renseignements personnels officielles pour ensuite devenir chef des Services d'information. De 1989 à 2004, il a occupé diverses fonctions au Commissariat à la protection de la vie privée du Canada et il a terminé sa carrière comme directeur adjoint, Évaluation des facteurs relatifs à la vie privée (EFVP). Dans ce poste, Claude Beaulé a joué un

Biographies

Chair : Mr. Blair Stewart

Blair Stewart is Assistant Privacy Commissioner of New Zealand. Mr. Blair worked in a commercial law firm in Auckland before joining the Office of the Privacy Commissioner when it was established in New Zealand in 1993. His roles include privacy policy, codes of practice, technology and international issues. Mr. Stewart has contributed to international privacy work through the Asia Pacific Privacy Authorities Forum and as a member of the APEC ECSG Data Privacy Subgroup since its inception. He has focussed on developing flexible and effective regulatory and institutional mechanisms for protecting privacy at national and supra-national level. Since 1996 Blair Stewart has promoted privacy impact assessment as a flexible tool for decision-makers and regulators dealing with novel and complex technological challenges to privacy. In 2002 Mr. Stewart wrote a *Privacy Impact Assessment Handbook* which has been influential in New Zealand and elsewhere. He holds a B.A. and LL.B.(Hons) from the University of Auckland and has been admitted as a Barrister and Solicitor of the High Court of New Zealand and as a Solicitor of the Supreme Court of England and Wales.

Chairs

Mr. Claude Beaulé

Claude Beaulé is a privacy consultant who began his privacy career in 1978 at the National Archives of Canada, first in responding to formal personal information requests and, later, as Chief of Information Services. From 1989 to 2004, Claude Beaulé served in various positions in the Office of the Privacy Commissioner of Canada, culminating as Acting Director of Privacy Impact Assessments (PIAs). In this position, Mr. Beaulé was instrumental in educating and establishing a rapport with privacy staff to help them conduct PIAs, including identifying privacy risks and

rôle actif pour établir des relations avec le personnel affecté à la protection de la vie privée afin de les aider à faire des évaluations des facteurs relatifs à la vie privée – et de les former dans ce domaine – de même qu'à cerner les risques et à élaborer des stratégies d'atténuation. Depuis qu'il a pris sa retraite, il travaille comme spécialiste de la protection des renseignements personnels auprès de la Division des politiques de l'information et de la protection des renseignements personnels, du Secrétariat du Conseil du Trésor, et au Commissariat à la protection de la vie privée. En 2005, il a reçu le Prix d'excellence pour l'ensemble de ses réalisations en matière d'accès à l'information et de protection de la vie privée, en reconnaissance de ses réalisations spéciales, de son engagement et de son dévouement dans ce domaine tout au cours de sa carrière. Claude Beaulé a terminé son cours d'informatique au cégep de Hull, au Québec (Canada), en 1972.

M. LeRoy Brower

LeRoy Brower est directeur, *Health Information Act* (*HIA*, Loi sur les renseignements sur la santé) au Bureau du commissaire à l'information et à la protection de la vie privée de l'Alberta. Au cours des cinq dernières années, il a dirigé l'équipe de la santé pour l'aider à assurer la surveillance de l'*HIA*, y compris les enquêtes menées sur les plaintes relatives à la protection de la vie privée, les demandes de médiation liées aux examens aux termes de l'*HIA* et de la *Federal Information and Protection of Privacy Act* (*FOIP*); il lui a aussi prêté son concours pour examiner les évaluations des facteurs relatifs à la vie privée soumises au commissaire, et les commenter. Il a occupé divers postes liés à l'application de la *FOIP* au gouvernement de l'Alberta : coordonnateur de la *FOIP*, Affaires municipales, conseiller en matière de *FOIP*, Environnement et Énergie et coordonnateur de la *FOIP* aux Services sociaux. Avant d'occuper des fonctions liées à la *FOIP* et à l'*HIA*, il a travaillé aux Services sociaux comme enquêteur sur les mauvais traitements infligés aux enfants.

M. David Flaherty, Ph. D.

David Flaherty est spécialiste des questions de gestion des politiques sur l'information et la protection de la vie privée. Il a été le premier

developing mitigation strategies. Since retiring, Mr. Beaulé has worked as a privacy specialist with the Information and Privacy Policy Division of the Treasury Board Secretariat and the Office of the Privacy Commissioner. In 2005, Mr. Beaulé received a government Access to Information and Privacy Lifetime Achievement Award to recognize his special achievements, commitment and dedication in the field of privacy throughout his career. Claude Beaulé completed a Computer Science course at the CEGEP de Hull, Québec, Canada in 1972.

Mr. LeRoy Brower

LeRoy Brower is the Director, Health Information Act (HIA) for the Office of the Information and Privacy Commissioner of Alberta. Over the past five years he has led the health team in providing oversight of the HIA, including investigating privacy complaints, mediating request for reviews under the HIA and Freedom of Information and Protection of Privacy Act (FOIP), and reviewing and commenting on privacy impact assessments submitted to the Commissioner. Mr. Brower has held FOIP positions in the Alberta Government as FOIP Coordinator, Municipal Affairs; FOIP Advisor, Environment & Energy; and FOIP Coordinator, Social Services. Prior to LeRoy Brower's work with the FOIP and HIA legislation, he was a child abuse investigator for Social Services.

Dr. David Flaherty

David Flaherty is a specialist in the management of privacy and information policy issues. He served as British Columbia's first Information and

commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique (1992-1999) et il est actuellement membre du Comité consultatif externe du Commissariat à la protection de la vie privée du Canada et conseiller en chef en matière de protection des renseignements personnels de l'Institut canadien d'information sur la santé. À titre de consultant, il donne des conseils stratégiques sur la gestion de questions relatives à la protection des renseignements personnels et sur les relations avec les autorités, les avocats et le grand public dans ce domaine. De plus, il évalue la conformité en matière de protection des renseignements personnels, prépare des évaluations des facteurs relatifs à la vie privée, gère les atteintes à la protection de la vie privée et élabore des plans de gestion de la protection des renseignements personnels. David Flaherty a commencé son travail dans ce domaine en tant qu'adjoint de Alan Westin à l'Université Columbia, en 1964. En 1974, il commence son travail de politique publique comparée en Europe et en Amérique du Nord, qui l'amène à publier plusieurs livres dont *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (1989). Il a publié ou révisé 14 ouvrages. Il est titulaire d'un diplôme de l'Université McGill (1962) et il a obtenu sa maîtrise et son doctorat à l'Université Columbia. Il a enseigné dans plusieurs universités canadiennes, à l'Université Princeton et à l'Université de Virginia.

M. Donald Lemieux

Donald Lemieux est Directeur exécutif, Politique de l'information, de la protection des renseignements personnels et de la sécurité, au Secrétariat du Conseil du Trésor. Avant de se joindre au Secrétariat du Conseil du Trésor du Canada, en 2001, à titre de conseiller principal en politique, il a occupé divers postes supérieurs au gouvernement, dont ceux de directeur de l'accès à l'information et à la protection des renseignements personnels au ministère des Communications et de conseiller juridique de la Division du droit à l'information et à la protection des renseignements personnels et du Groupe d'étude de l'accès à l'information, au ministère de la Justice. Depuis juin 2004, il gère les politiques du gouvernement du Canada sur l'accès à l'information, la protection de la vie privée, la protection des données et la divulgation proactive.

Privacy Commissioner (1992-99) and is currently a member of the External Advisory Committee to the Privacy Commissioner of Canada and the Chief Privacy Advisor to the Canadian Institute for Health Information. As a consultant, Dr. Flaherty provides strategic advice on the management of privacy issues and relationships with privacy authorities, advocates, and the general public; assessing privacy compliance; preparing Privacy Impact Assessments; managing privacy breaches; and developing privacy management plans. He began his privacy work as an assistant to Alan Westin at Columbia University in 1964. In 1974 he started comparative public policy work in Europe and North America that led to a series of books, including *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (1989). David Flaherty has written or edited 14 books. He is a graduate of McGill University (1962) and has an MA and Ph.D. from Columbia University. He has taught at several Canadian universities and at Princeton University and the University of Virginia.

Mr. Donald Lemieux

Donald Lemieux is Executive Director, Information, Privacy and Security Policy for the Treasury Board Secretariat. Before joining the Treasury Board of Canada Secretariat in 2001 as a Principal Policy Advisor, Donald Lemieux held a number of senior government positions, including Director of Access to Information and Privacy with the Department of Communications, Legal Advisor in the Department of Justice's Information Law and Privacy Division and the Access to Information Review Task Force. Since June 2004, Mr. Lemieux has managed the Government of Canada's policies on access to information, privacy, data protection and proactive disclosure, and provided strategic advice to Ministers and government departments. In his current position, he provides policy direction to ensure Canadians' rights to government information are balanced with the govern-

Il donne aussi des conseils stratégiques aux ministres et à divers ministères. Son poste actuel l'amène à formuler des orientations stratégiques pour faire en sorte que les droits des Canadiennes et Canadiens en matière d'information gouvernementale tiennent compte de l'obligation du gouvernement de protéger les données confidentielles. Il a également dirigé de nombreuses initiatives gouvernementales d'importance, y compris la politique de sécurité gouvernementale, la gestion d'identité, l'accès des personnes handicapées aux services gouvernementaux et l'uniformité des sites Web du gouvernement. Donald Lemieux est avocat, membre du Barreau du Haut-Canada; il est spécialiste des renseignements fédéraux et du droit relatif au respect de la vie privée.

ment's obligation to protect sensitive data. Mr. Lemieux has also led a number of key government initiatives including government security policy, identity management, disabled persons' access to government services, and uniformity of government web sites. Donald Lemieux is a lawyer and a member of the Law Society of Upper Canada, specializing in federal information and privacy law.

M^{me} Rebecca Richards

En tant que directrice de la conformité en matière de vie privée au Bureau de la vie privée du département de la Sécurité intérieure, Rebecca J. Richards est chargée d'élaborer des politiques et de veiller, pour le compte du département et de ses composantes, au respect des exigences liées aux évaluations des facteurs relatifs à la vie privée, aux notifications relatives aux systèmes de tenue des dossiers et des autres exigences connexes en matière de protection de la vie privée. Avant de travailler au département de la Sécurité intérieure, M^{me} Richards était la directrice de Policy and Compliance (Politique et Conformité) d'une organisation qui offrait un programme indépendant et sans but lucratif d'attestation de la confidentialité aux entreprises qui font des affaires sur le Web. Elle a également travaillé comme spécialiste internationale du commerce au département du Commerce des États-Unis et a contribué à la préparation de l'accord États-Unis–Europe sur la sphère de sécurité. Elle a obtenu un B.A. à l'Université du Massachusetts (Amherst), ainsi qu'une maîtrise en commerce international et en politique de placement et une maîtrise en administration des affaires à l'Université George Washington.

Ms. Rebecca Richards

As the Director of Privacy Compliance at the Department of Homeland Security, Rebecca J. Richards is responsible for developing policies and ensuring compliance with requirements for privacy impact assessments, system of records notices, and other associated privacy requirements for the Department and its components. Before joining DHS, Richards was Director of Policy and Compliance at and independent non-profit privacy certification program for companies doing business on the web. She has also worked as an international trade specialist with the U.S. Department of Commerce and worked on the U.S. – European Union Safe Harbor accord. She received her B.A. from University of Massachusetts, Amherst, a Masters in international trade and investment policy and an MBA from George Washington University.

M. Trevor Shaw

Trevor Shaw est comptable agréé et consultant certifié en gestion. Pendant 30 ans, il a effectué la vérification de la gestion des ministères et organismes gouvernementaux, tant à l'échelon

Mr. Trevor Shaw

Trevor Shaw is a Chartered Accountant and Certified Management Consultant. For 30 years he audited Canadian government departments and agencies at both federal and provincial levels. His

fédéral qu'à l'échelon provincial. Son travail consistait notamment à faire des vérifications du rendement, des vérifications comptables, des vérifications en matière de protection des renseignements personnels et à passer en revue les évaluations des facteurs relatifs à la vie privée. En décembre 2004, M. Shaw a été nommé directeur général par intérim de la Direction de la vérification et de la revue du Commissariat à la protection de la vie privée du Canada. Il a la responsabilité de développer la capacité de vérification du Commissariat et de diriger les vérifications des ministères et organismes fédéraux visant à évaluer la conformité à la *Loi sur la protection des renseignements personnels*, de même que les vérifications des entités du secteur privé assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques*. Sa Direction est également chargée d'analyser les évaluations des facteurs relatifs à la vie privée rédigées par les ministères et organismes fédéraux. Avant de faire de la vérification législative, Trevor Shaw était associé dans un cabinet comptable national.

work has included performance and financial auditing, privacy auditing and reviewing privacy impact assessments.
In December 2004 Trevor Shaw was appointed Acting Director General for the Audit & Review Branch of the Office of the Privacy Commissioner of Canada. He is responsible for developing the Office's audit capacity and capabilities and leading audits of federal departments and agencies to assess compliance with the *Privacy Act* , as well as private sector entities subject to the *Personal Information Protection and Electronics Documents Act*. His branch is also responsible for reviewing Privacy Impact Assessments completed by federal departments and agencies. Prior to legislative auditing, Mr. Shaw was a partner in a national accounting firm.

M. Mark Vale

Mark Vale a été nommé en juillet 2006 à titre de premier directeur général de l'information et de la protection de la vie privée, au ministère des Services gouvernementaux de l'Ontario. Il dirige l'élaboration et la mise en application de stratégies de gestion de l'information gouvernementale qui soutiennent de solides pratiques commerciales, appuient la capacité du gouvernement et font de l'accès à l'information et de la protection des renseignements personnels des considérations commerciales essentielles. Avant d'entrer dans la fonction publique ontarienne, Mark a été président de Information Management & Economics Inc. où il a aidé des administrations publiques et des sociétés d'un bout à l'autre du Canada à gérer plus efficacement l'information et les ressources en matière de connaissances. C'est un économiste de l'information qui possède plus de 25 ans d'expérience de la politique, de la stratégie et de la planification en matière d'information de même que de la mise en œuvre de programmes de gestion des connaissances et d'information gouvernementale. Il figure parmi les leaders en Amérique du Nord dans le domaine de la gestion des connaissances et de l'information et il a enseigné à l'Université de l'Alberta, à l'Université

Mr. Mark Vale

Mark Vale was appointed the first Chief Information and Privacy Officer for the Ontario Ministry of Government Services in July 2006. He leads the governments' development and implementation of information management strategies that support sound business practices, build government capacity, and make access to information and privacy fundamental business considerations. Before joining the Ontario Public Service, Mark Vale was President of Information Management & Economics, Inc. helping governments and companies across Canada more effectively manage information and knowledge resources. Mr. Vale is an information economist with more than 25 years experience in information policy, strategy and planning, and implementing corporate information and knowledge management programs. He is one of North America's leaders in shaping the information and knowledge management disciplines and has taught at the University of Alberta, York University, Stanford University and California State University. Born in Toronto, Mark Vale received his MA in economics from the University of California, Berkeley and his Ph.D. from Stanford University.

York, à l'Université Stanford et à l'Université d'État de la Californie. Né à Toronto, il détient une maîtrise en économie de l'Université de Californie, à Berkeley, et un doctorat de l'Université Stanford.

M. Nigel Waters

Nigel Waters est directeur chez Pacific Privacy Partners. Depuis 1997, il est conseiller à plein temps en matière de conformité aux lois relatives à la vie privée auprès d'administrations publiques et d'entreprises en Australie, en Nouvelle-Zélande, à Hong Kong et aux États-Unis. Son remarquable travail d'évaluation des facteurs relatifs à la vie privée a été déterminant dans le projet de carte à puce mis en œuvre par le gouvernement de Hong Kong et dans le projet d'authentification en ligne du gouvernement de la Nouvelle-Zélande. Avant 1997, M. Waters avait travaillé pendant 12 ans comme cadre supérieur à la mise en application de lois sur la vie privée et la protection des renseignements personnels à titre de commissaire adjoint de la vie privée en Australie (1989-1997) et de registraire adjoint de la protection des données au Royaume-Uni (1985-1989). Il a été rédacteur en chef adjoint de *Privacy Law & Policy Reporter* (1997-2005) et il est actuellement membre du comité exécutif du Consumers Federation of Australia et chercheur principal du projet d'interprétation des principes de la vie privée confié au Cyberspace Law & Policy Centre, à l'Université de New South Wales. M. Waters est titulaire de maîtrises de l'Université Cambridge, de l'Université de Pennsylvanie et de l'Université de Technology à Sydney.

Mr. Nigel Waters

Nigel Waters is a director at Pacific Privacy Partners. Since 1997 Nigel Waters has been a full-time consultant on compliance with privacy laws to governments and businesses in Australia, New Zealand, Hong Kong and the United States. His notable privacy impact assessment work has been significant PIAs for the Hong Kong Government's smartcard ID card and the New Zealand Government's on-line authentication project. Prior to 1997, Mr. Waters has 12 years experience at senior executive level of implementing privacy and data protection laws particularly as Australia's Deputy Privacy Commissioner (1989-97) and as Assistant Data Protection Registrar, UK (1985-89). Nigel Waters was Associate Editor of *Privacy Law & Policy Reporter* (1997-2005) and is currently on the Executive of the Consumers Federation of Australia and Principal Researcher to the Interpreting Privacy Principles Project at the Cyberspace Law & Policy Centre at the University of New South Wales. Mr. Waters holds Masters Degrees from Cambridge University, the University of Pennsylvania and the University of Technology Sydney.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Évaluation des facteurs relatifs à la vie privée : enjeux et approches pour les organismes de réglementation

Privacy Impact Assessment: Issues and Approaches for Regulators

Par/by:

Blair Stewart

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

* L'auteur désire remercier Nigel Waters et David Flaherty pour leurs précieux commentaires sur les premières versions de ce texte.

[traduction] *Les évaluations des facteurs relatifs à la vie privée (ÉFVP) sont sorties du brouillard des débuts et sont maintenant chose courante. Les prochaines années montreront si elles entraîneront l'émergence des enjeux, la participation du public et une approche multilatérale aux initiatives de développement visant la protection de la vie privée, et si elles réussiront à équilibrer les intérêts opposés qui sont plus sensibles à la protection de la vie privée qu'ils ne l'étaient au cours des trente dernières années du XX^{e} siècle.*
Roger Clarke, *A History of Privacy Impact Assessments*, 2004[1]

Résumé

Le présent document décrit les objectifs d'un atelier au cours duquel on examinera la perspective des organismes de réglementation sur l'évaluation des facteurs relatifs à la vie privée (ÉFVP). Le document et l'atelier sont conçus de façon à analyser le processus d'ÉFVP en quatre parties :

- *le démarrage* – le rôle des organismes de réglementation au début de l'évaluation;
- *l'exécution* – les problèmes que rencontrent les organismes de réglementation au cours de l'évaluation;
- *les résultats* – lorsqu'on reçoit le rapport d'évaluation des facteurs relatifs à la vie privée;
- *la valeur* – la valeur de l'évaluation comme outil de réglementation.

L'atelier vise à explorer ces sujets d'une façon qui permettra aux participants d'améliorer leur compréhension des enjeux et de répondre aux questions posées dans le document. Il mettra l'accent sur le partage des expériences pratiques — ce qui fonctionne et ce qui ne fonctionne pas — afin de mettre au jour les forces et les embûches du processus pour les organismes de réglementation. Pour utiliser l'imagerie du thème de la Conférence, nous espérons suggérer où on pourrait installer des phares afin d'éviter aux organismes de réglementation de naviguer dans des océans inconnus et d'y faire naufrage.

* The author acknowledges the helpful comments of Nigel Waters and David Flaherty on drafts of this paper.

"PIAs have emerged from an early fog, and are now mainstream. The coming years will tell whether they force the surfacing of issues, the involvement of the public, and a multi-stakeholder approach to development initiatives that reflects the privacy interest, and achieves balances among conflicting interests that are less privacy-insensitive than was the case during the last three decades of the twentieth century."

Dr Roger Clarke, *A History of Privacy Impact Assessments*, 2004[1]

Synopsis

This paper outlines the objectives of a workshop examining the regulators' perspective on privacy impact assessment (PIA). The paper and workshop are structured to move through the PIA process under four headings:

- *Getting started* – the regulator's role at the outset
- *Getting through* – the issues for regulators while conducting an assessment
- *Getting results* – when the privacy assessment report arrives
- *Getting value* – how the process measures up as a regulatory tool.

The workshop aims to explore the topics in a way that improves participants' understanding of the issues, and answers the questions posed in the paper. The workshop will emphasize sharing practical experiences–what works and what doesn't–to find the regulatory strengths and pitfalls of the process. To use the imagery of the conference theme, we hope to suggest where navigation lights might be sited to ensure that regulators don't sail into uncharted waters, then off the edge of the world.

We anticipate that this issues paper may be supplemented by several additional resource papers and case studies that cover each of the four parts of the workshop.

Nous nous attendons à ce que le présent document de travail soit complété par plusieurs autres documents ressources et des études de cas pour chacune des quatre parties de l'atelier.

Introduction

Au cours de la dernière décennie, l'évaluation des facteurs relatifs à la vie privée (ÉFVP) est passée du statut d'idée intéressante à celui de réalité concrète. Elle fait maintenant partie intégrante, dans plusieurs juridictions, de la gestion moderne de la protection de la vie privée. Les organismes de réglementation peuvent s'en servir et elle a tout aussi fréquemment recours aux ressources des organismes de réglementation.

Dans son discours d'ouverture de la 22e Conférence internationale des commissaires à la protection des données et de la vie privée, tenue à Venise en 2000, David Flaherty décrivait l'ÉFVP comme [traduction] « un outil essentiel » à la protection des données[2]. À la suite de la 25e Conférence internationale tenue à Sydney, en Australie, la commissaire à la protection de la vie privée de Nouvelle-Zélande a animé, à titre d'activité annexe, un atelier international sur l'évaluation des facteurs relatifs à la vie privée[3].

Il n'est pas étonnant que les organismes de réglementation de la protection de la vie privée s'intéressent à l'ÉFVP ou que la Conférence traite à nouveau de ce sujet. Le modèle de commissaire à la protection des données ou à la protection de la vie privée représente dans son essence même une autorité de réglementation polyvalente. Tous les organismes de protection des données inscrits à la Conférence possèdent de multiples rôles couvrant des fonctions de consultation, d'éducation, d'enquête et de règlement de conflits. Bon nombre ont d'autres pouvoirs et d'autres fonctions comme l'élaboration de règlements et la vérification de la conformité avant et après le fait. La réglementation de la vie privée exige une grande capacité d'adaptation et d'innovation, et nombreux sont ceux qui ont trouvé dans l'ÉFVP un complément utile à leur « boîte à outils sur la vie privée ».

Au cours des années, un certain nombre de séances tenues sur l'ÉFVP lors de symposiums ou de conférences ont porté sur des questions fondamentales comme les suivantes :

- Qu'est-ce que l'ÉFVP?

Introduction

In the last decade, Privacy Impact Assessment (PIA) has moved from being an interesting idea to a practical reality. It is now an integral part of modern privacy management in several jurisdictions and one that regulators may draw upon or, just as frequently, one that draws upon the resources of regulators.

David Flaherty's keynote address to the 22nd International Conference of Data Protection and Privacy Commissioners in Venice (2000) described PIA as "an essential tool" for data protection.[2] Following the 25th International Conference in Sydney, the New Zealand Privacy Commissioner hosted an International Workshop on Privacy Impact Assessment as a related event.[3]

It is not surprising that privacy regulators should be interested in PIA or that the conference should return to the subject. The data protection or privacy commissioner model is quintessentially a multi-faceted regulator. All data protection authorities accredited to the conference have multiple roles spanning advisory, educational, investigative functions and dispute resolution. Many have additional powers and functions such as rule-making and prior and post-facto compliance checking. Privacy regulation has required adaptability and innovation and many have found PIA a flexible adjunct to their "privacy toolkit".

Over the years a number of PIA symposia or conference sessions have tended to focus on such fundamental questions as:

- What is PIA?
- What are the advantages of PIA?
- What are the disadvantages?

Discussion then usually proceeds to how best to design processes to introduce PIA into an organization, government or jurisdiction. The perspective has been from the interests of both potential users of PIA and the needs of the potential assessors. For potential users, what are the advantages for my organization? How would I introduce PIA? For assessors, how would I undertake an assessment? What standards or guidelines should I follow?

With PIA now mandated or operational in several jurisdictions, it is time to focus on the regulators' role. Although the fundamental "why" and "how" questions are by no means all resolved, this work-

- Quels sont les avantages de l'ÉFVP?
- Quels sont ses désavantages?

En général, la discussion portait ensuite sur la meilleure façon de concevoir des processus visant à introduire l'ÉFVP dans un organisme, une administration ou une juridiction. Le point de vue adopté était celui de l'intérêt des utilisateurs potentiels de l'ÉFVP et des besoins des évaluateurs éventuels. Les utilisateurs potentiels voulaient savoir quels étaient les avantages pour leur organisation et comment ils pouvaient y introduire l'ÉFVP. Les évaluateurs se demandaient comment ils pouvaient entreprendre une évaluation et quelles normes ou lignes directrices ils devaient suivre.

Comme l'ÉFVP est maintenant obligatoire ou opérationnelle dans plusieurs juridictions, il est temps de se centrer sur le rôle des organismes de réglementation. Même si les questions fondamentales du pourquoi et du comment ne sont certainement pas toutes réglées, cet atelier prend le risque de considérer que la place de l'ÉFVP est maintenant assurée. En conséquence, nous nous emploierons à définir le rôle des organismes de réglementation dans l'ÉFVP et à chercher des façons de minimiser les problèmes de réglementation et à maximiser les avantages.

Quelques postulats pour le travail en atelier

Il y a suffisamment de questions liées à l'ÉFVP et aux expériences collectives pour occuper une journée entière sans difficulté. Avec seulement deux heures, le défi est de limiter le centre d'intérêt. Il faudra conserver certains sujets pour une autre occasion.

Modèles d'ÉFVP
Il existe un grand nombre de modèles d'ÉFVP en usage dans diverses régions. Certains sont requis par la loi ─ qui exige qu'une ÉFVP soit entreprise dans certaines circonstances —, alors que d'autres sont obligatoires aux termes des politiques d'un gouvernement ou d'une entreprise, ou sont entièrement volontaires. Un grand nombre de schémas sont centrés sur un secteur particulier — généralement le secteur public ou la santé — alors que d'autres s'efforcent d'inclure toutes les organisations d'une économie. La discussion en atelier n'exclut aucun modèle.

shop might risk taking the case for PIA for granted. Therefore, we will focus on identifying privacy regulators' roles in PIA, and seeking ways to minimize the regulatory problems and maximize the benefits.

Some presumptions for the workshop

There are enough issues surrounding PIA and collective experiences to fill an entire day without difficulty. With just two hours the challenge is to keep the focus limited. Some issues must be left for another occasion.

PIA models
There are a variety of PIA models operating in different jurisdictions. Some are mandated by law – requiring PIAs to be undertaken in certain circumstances – while others are required under government or company policy, or are entirely voluntary. Many schemes focus upon a particular sector – typically public sector or health – while others seek to embrace all organizations in an economy. No model is excluded from the workshop discussion.

However, the workshop assumes a model in which the regulator is at arm's length from the assessor. In other words, the workshop will not examine the challenges of privacy commissioners conducting assessments themselves, as some do, where the issues may be similar to those faced by any other assessor. This session is interested in the commissioner (or other entity) *as regulator* (and as consumer of completed privacy impact reports).

Participation – meaning of "regulator"
The majority of regulators at the workshop are, naturally enough, likely to be privacy and data protection authorities accredited to the conference. Other regulators such as those in specialized areas of, say, e-government, consumer or financial regulation, are also welcome. Indeed, for this workshop we suggest an expansive view of regulator which may encompass some internal control officers (typically Chief Privacy Officers) in companies and government departments. Also included are those who are at arms-length from the proposals being evaluated and the assessment being conducted, but who have some general or specific responsibility to ensure a level of privacy compliance in the PIA process. This could encompass, for instance, government coordinating ministries

Cependant, l'atelier postule que, dans le modèle, l'évaluateur n'a pas de lien de dépendance vis-à-vis de l'autorité de réglementation. En d'autres mots, l'atelier n'étudiera pas les défis auxquels font face les commissaires à la protection de la vie privée qui réalisent eux-mêmes les évaluations, comme certains le font, parce que dans cette situation, les problèmes auxquels ils font face peuvent être semblables à ceux de n'importe quel évaluateur. Cet atelier s'intéresse au commissaire (ou à une autre entité) *en tant qu'organisme de réglementation* (et en tant que consommateur de rapports d'évaluation des facteurs relatifs à la vie privée).

Participation – signification de l'expression « organisme de réglementation »
La majorité des organismes de réglementation représentés à l'atelier seront probablement, et logiquement, les organismes de protection des données et de la vie privée inscrits à la Conférence. D'autres organismes de réglementation, comme ceux des domaines spécialisés, par exemple, du gouvernement électronique, de la protection des consommateurs ou de la réglementation financière, sont aussi les bienvenus. En effet, pour cet atelier, nous proposons une vision élargie de l'organisme de réglementation, qui peut englober certains agents de contrôle interne (en général des chefs de la protection des renseignements personnels) dans des entreprises et des ministères. Cette vision englobe aussi ceux qui sont indépendants des propositions évaluées et de l'évaluation en cours, mais qui sont chargés, directement ou indirectement, d'assurer au processus d'ÉFVP un certain niveau de conformité aux règles de protection de la vie privée. Il pourrait s'agir, par exemple, de ministères qui coordonnent ou financent les ÉFVP obligatoires (p. ex. comme exigence éthique dans la recherche en santé) ou comme condition de financement (p. ex. pour le développement de nouveaux systèmes d'information) lorsque ces organisations jouent des rôles assimilables à celui d'un organisme de réglementation concernant la conformité aux règles ou aux bonnes pratiques de protection de la vie privée.

Participation – autres
Nous postulons que tous les participants seront familiers avec l'ÉFVP et travailleront dans un environnement qui utilise l'ÉFVP ou envisage de l'adopter. Cet atelier n'est *pas* conçu comme une introduction à l'ÉFVP. Étant donné le sujet central

or funding departments that require PIA by policy (e.g. as an ethical requirement for health research) or as a condition of funding (e.g. for developing new information systems) when those organizations perform regulator-like roles on privacy compliance or good privacy practice.

Participation – others
We assume that all participants will be familiar with PIA and operating in an environment that is using or contemplating adopting PIA. This is *not* a workshop designed to introduce people to PIA. The majority of participants are expected to be from regulators given the prime focus of the workshop. However, it will enrich the workshop to have non-regulators who are familiar with working with or observing regulators. For instance, participants such as expert assessors or client organizations who have previously commissioned or undertaken PIAs are welcome. Such participants may be able to inform the workshop about such things as regulatory choices that impact in a positive or negative sense on organizations.

Balance of the Issues Paper

The balance of the paper tracks the process of PIA from start to finish with a final part devoted to overall questions of success or failure of the regulatory model.

The four parts are:
- Getting started – the regulator's role at the outset
- Getting through – the issues for regulators while conducting an assessment
- Getting results – when the privacy assessment report arrives
- Getting value – how the process measures up as a regulatory tool.

The whole workshop is intended to be fluid and participatory. Long presentations are not contemplated and will not be allowed. There will be short papers on each of the four topic areas as take away resources. Within each session one or two discussion leaders have been identified to 'kick-start' discussion with some relevant insights and short case studies before drawing all participants in the discussion. We hope that everyone will leave with a better understanding of the problem areas and with some strategies for making the most of PIA.

de l'atelier, on s'attend à ce que la majorité des participants viennent d'organismes de réglementation. Cependant, la présence de personnes qui ne viennent pas d'organismes de réglementation mais qui connaissent le travail de ceux-ci ou sont habituées à les observer constituera un enrichissement pour l'atelier. Ainsi, des participants comme des évaluateurs experts ou des représentants d'organisations clientes ayant déjà financé ou entrepris des ÉFVP sont les bienvenus. Ces participants pourraient amener à l'atelier des renseignements sur des éléments comme les choix réglementaires qui ont des répercussions positives ou négatives sur les organisations.

Le reste du document de travail

Le reste du document retrace le processus d'ÉFVP du début jusqu'à la fin. La dernière partie est consacrée aux questions générales du succès ou de l'échec du modèle réglementaire.

Les quatre parties sont les suivantes :

- le démarrage – le rôle des organismes de réglementation au début de l'évaluation;
- l'exécution – les problèmes que rencontrent les organismes de réglementation au cours de l'évaluation;
- les résultats – lorsqu'on reçoit le rapport d'évaluation des facteurs relatifs à la vie privée;
- la valeur – la valeur de l'évaluation comme outil de réglementation.

L'atelier a été conçu de façon à être fluide et à encourager la participation. Les longues présentations ne font pas partie de ce concept et ne seront pas autorisées. On distribuera de courts documents traitant de chacun des sujets comme ressources à conserver. Pour chaque séance, on a nommé un ou deux animateurs, chargés de faire démarrer la discussion à l'aide de propos pertinents et de courtes études de cas avant d'englober tous les participants dans la discussion. Nous espérons que tous les participants en tireront une meilleure compréhension des enjeux et certaines stratégies visant à faire la meilleure utilisation possible des ÉFVP.

Part A: Getting started

Privacy impact assessment doesn't simply "happen", someone makes it happen.

In a particular case this is typically through either:

- the application of a pre-determined rule–such as requiring certain projects over $50,000 to undergo PIA, or
- exercise of judgment on an *ad hoc* basis–"I think this project warrants a PIA".

Sometimes there will be an expectation of completing a PIA as a condition of doing business in a regulated privacy environment.

Considering a PIA, or deciding to undertake one, may trigger a series of further decisions for which there may or may not be pre-determined rules. Examples include whether to do further investigations before committing to a full PIA, setting terms of reference, choosing an assessor or assembling a team, and setting a timeline.

Aspects of all of these may–but need not–involve a regulator. For instance, one jurisdiction's regulator may have set the rule that PIAs are mandatory but the regulator is otherwise not involved. In other jurisdictions the rules may be less rigid but the regulator may be consulted on the decision to undertake an assessment. Several jurisdictions have model PIA templates of varying quality.

Questions for discussion:

- What roles do regulators currently perform?
- Are all of these appropriate? Why so? Why not?
- Should they perform further roles?
- What problems do they encounter in these roles?
- What are the priorities for regulators at this stage?
- What regulatory action most contributes to successful outcomes?
- What causes the most problems?
- Are we requiring PIA in the right cases? Or do our systems miss some important cases? Or do we require PIA when it is really not warranted?
- Quality control and appropriate scope of an assessment are clearly important considerations at the outset if the process is to be of value – how can they be ensured?

Partie A : Le démarrage

L'évaluation des facteurs relatifs à la vie privée ne se fait pas toute seule; il faut que quelqu'un la réalise.

Sur le plan concret, l'évaluation se fait généralement, soit :

- par l'application d'une règle prédéterminée — comme l'obligation que certains projets de plus de 50 000 dollars soient soumis à une ÉFVP;
- par l'exercice du jugement sur une base ponctuelle — « Je crois que ce projet devrait faire l'objet d'une ÉFVP ».

Dans un environnement de protection de la vie privée, il pourra arriver qu'on s'attende à ce qu'une ÉFVP soit effectuée comme condition d'obtention d'un contrat.

Le fait d'envisager la réalisation d'une ÉFVP ou de décider d'en effectuer une peut déclencher une série de décisions subséquentes pour lesquelles il peut exister des règles prédéterminées ou non. Mentionnons, à titre d'exemple, le fait de décider s'il faut effectuer d'autres recherches avant de s'engager dans une ÉFVP complète, définir un mandat, choisir un évaluateur ou former une équipe, et établir un échéancier.

Certains aspects de toutes ces questions pourraient — mais ne doivent pas nécessairement — impliquer un organisme de réglementation. Par exemple, l'organisme de réglementation d'une juridiction peut avoir adopté la règle que les ÉFVP sont obligatoires, mais que l'organisme n'a rien à voir avec celles-ci. Dans d'autres juridictions, les règles peuvent être moins rigides, mais l'organisme peut être consulté sur la décision d'entreprendre une évaluation. Plusieurs juridictions ont des modèles d'ÉFVP de qualités variables.

Questions pour alimenter la discussion

- Quels rôles les organismes de réglementation jouent-ils actuellement?
- Ces rôles sont-ils tous appropriés? Si oui, pourquoi? Si non, pourquoi?
- Devraient-ils jouer d'autres rôles?
- À quels problèmes font-ils face dans ces rôles?
- Quelles sont les priorités pour les organismes de réglementation à ce stade?
- Quelle mesure réglementaire contribue le plus

Part B: Getting through

PIA of the typical model assumed in this workshop is performed not by the regulator but by another person or team typically answering to the organization whose project is being assessed. So what if any role does or should a regulator play? Is it useful to be in touch with an assessor or does this affect the arms-length relationship of assessor and regulator? Can interim contact lead to the regulator being burdened with requests for *ad hoc* advice or opinions when the PIA's purpose is to make a more systematic and scientific assessment of privacy impacts? On the other hand, if the regulator is entirely uninvolved during an assessment, will that defer problems until it is too late to influence events? Does close involvement compromise the regulator?

Questions for discussion:

- What roles do regulators currently perform?
- Are all of these appropriate?
- Should they perform further roles?
- What problems do they encounter in these roles?
- What are the regulators' priorities at this stage?
- What regulatory action most contributes to successful outcomes?
- In the interactions between regulator and assessor, what works well for assessors? For regulators? For organizations? What causes most problems?

Part C: Getting results

Any PIA process delivers a report on the findings and recommendations at some point. Depending on local practices this may come to the regulator; perhaps in draft form with opportunity to comment, or perhaps just for information. There may be different views on which approach is most effective from a regulatory perspective.

The reports to regulators may range from projects of major national importance to systems affecting just one company and its employees. Regulators will always have limited resources to devote to PIA work and there will be many other tasks competing for attention. How can under-resourced and busy regulators make the most of this stage of the work? Can classes of PIA be differentiated by their importance or the appropriate regulatory action and responses? Is the practice of receiving

au succès des évaluations?
- Qu'est-ce qui cause le plus de problèmes?
- Exigeons-nous une ÉFVP dans les cas appropriés? Notre système laisse-t-il passer des cas importants? Ou au contraire demandons-nous des ÉFVP lorsque ce n'est pas vraiment nécessaire?
- Le contrôle de la qualité et la délimitation appropriée du champ de l'évaluation sont des considérations importantes lors du démarrage si l'on veut que le processus soit utile — comment peut-on y voir?

Partie B : L'exécution

Une ÉFVP du modèle général utilisé dans cet atelier est réalisée non par l'organisme de réglementation, mais par une autre personne ou une autre équipe, généralement subordonnée à l'organisation dont le projet est soumis à l'évaluation. Dans ce contexte, l'organisme de réglementation a-t-il un rôle à jouer, et si oui, lequel? Est-il utile qu'il ait des contacts avec un évaluateur, ou bien cela a-t-il un effet sur l'indépendance de la relation entre l'évaluateur et l'organisme de réglementation? Les contacts dans l'intervalle peuvent-ils avoir pour effet que l'organisme de réglementation soit assailli de demandes de conseils ou d'opinions ponctuelles alors que l'objectif de l'ÉFVP est d'effectuer une évaluation systématique et scientifique des facteurs relatifs à la vie privée? Par ailleurs, si l'organisme de réglementation ne joue aucun rôle durant l'évaluation, cela va-t-il repousser les problèmes jusqu'à ce qu'il soit trop tard pour que l'organisme influe sur les événements? Une participation étroite compromet-elle l'organisme de réglementation?

Questions pour alimenter la discussion
- Quels rôles les organismes de réglementation jouent-ils actuellement?
- Ces rôles sont-ils tous appropriés?
- Devraient-ils jouer d'autres rôles?
- À quels problèmes font-ils face dans ces rôles?
- Quelles sont les priorités de l'organisme de réglementation à ce stade?
- Quelle mesure réglementaire contribue le plus au succès des évaluations?
- Dans les interactions entre l'organisme de réglementation et l'évaluateur, qu'est-ce qui fonctionne bien pour les évaluateurs? Pour les organismes de réglementation? Pour les

PIAs "for information" (but no analysis or action) a pragmatic and appropriate response or an abrogation of responsibility? What do organizations expect and want? What does the public and legislature expect? What can regulators do with the reports in an individual or systemic way? How much regulatory resource is sufficient to do a credible job?

Now that PIA has been operating for a number of years, there are often multiple PIA reports on the one system or inter-related systems. Does this pose special changes ? Can regulators track recommendations and systems changes?

Questions for discussion:
- What roles do regulators currently perform? Are all of these appropriate?
- How actively do regulators perform the role of receiving PIA reports? Do they sit back and wait or chase assessors? Should they?
- If offered an opportunity to critique a report, how is that performed? How resource intensive is the process? How thorough?
- What problems do they encounter in these roles?
- What talents are required to perform this kind of work?
- Should they perform further roles?
- What are the regulators' priorities at this stage?
- What regulatory action most contributes to successful outcomes?
- Are regulators making the most of the PIA reports they receive? If not, why is this and what can be done?
- Are regulators operating transparently? Are the results of PIAs made available by regulators or organizations to affected communities or those working in privacy management?

Part D: Getting value

DPAs are multi-faceted regulators with many tools and powers to call on. Are regulators using PIA in the right way and for the right projects? Are other tools sometimes more useful? Do PIAs make a difference in privacy outcomes? How do we know?

In our attempts to systemize privacy management through PIA and similar systems are we "dumbing down" the process to the point where it is not useful? Is Dr. Roger Clarke right when he observed:

organisations? Qu'est-ce qui cause le plus de problèmes?

Partie C : Les résultats

Tout processus d'ÉFVP donne éventuellement lieu à un rapport sur les constatations et les recommandations. Selon les pratiques locales, ce rapport peut être transmis à l'organisme de réglementation, peut-être sous forme de version préliminaire invitant les commentaires, ou peut-être uniquement à titre d'information. On peut avoir des opinions différentes sur l'approche la plus efficace du point de vue réglementaire.

Les rapports soumis à l'organisme de réglementation peuvent concerner des sujets variant de projets d'importance nationale majeure à des systèmes n'affectant qu'une seule entreprise et ses employés. Les organismes de réglementation n'auront toujours que des ressources limitées à consacrer à l'ÉFVP, et un grand nombre d'autres tâches se disputeront toujours leur attention. Comment des organismes très occupés et manquant de ressources peuvent-ils tirer le maximum de ce stade du travail? Est-il possible de classer les ÉFVP par catégories selon leur importance ou selon l'approche et les mesures réglementaires qu'il faut adopter? La pratique de recevoir les rapports sur les ÉFVP « pour information » (mais non pour analyse ni pour suite à donner) constitue-t-elle une réponse pragmatique et appropriée, ou plutôt un abandon de responsabilités? Qu'attendent et que veulent les organisations? Qu'attendent le public et l'assemblée législative? Que peuvent faire les organismes de réglementation avec ces rapports, considérés individuellement ou collectivement? Quelles ressources réglementaires faudrait-il pour accomplir un travail crédible?

Maintenant que les ÉFVP se font depuis un bon nombre d'années, on produit souvent plusieurs rapports d'ÉFVP sur un seul système ou sur des systèmes interconnectés. Cela pose-t-il des défis spéciaux? Les organismes de réglementation peuvent-ils faire le suivi des recommandations et des modifications apportées aux systèmes?

Questions pour alimenter la discussion

- Quels rôles les organismes de réglementation jouent-ils actuellement? Ces rôles sont-ils tous appropriés?
- À quel point les organismes de réglementation

> "*From the late 1990s onwards, PIAs were recognized by a succession of government agencies as an idea whose time had come. A large number of Guidelines were prepared, which have varying degrees of authority and influence. It is normal for the routinisation of procedures to result in fairly mindless procedures and documents. Many sets of Guidelines are of the nature of checklists, and can easily lead to the generation of guideline-compliant documents; whereas others are intentionally introductory and designed to stimulate constructive approaches to what are usually complex and multi-dimensional problems.*"
>
> Dr Roger Clarke, *A History of Privacy Impact Assessments*, 2004[4]

Are there lessons to be learned from other fields of regulatory endeavour, both within data protection and elsewhere, that might point the way to better assessing and ensuring value for the community and privacy?

Questions for discussion:

- What do regulators currently do to ensure PIA delivers value?
- How is this measured or tested?
- What more should be done individually or collectively?
- What regulatory action has been found to most contribute to successful outcomes?

Endnotes

[1] http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html#Conc

[2] David Flaherty, "Privacy Impact Assessments: An essential tool for data protection", 2000, available through http://www2.garanteprivacy.it/garante/prewiew/0,1724,1619,00.html?sezione=116&LANG=1 and at http://beta.austlii.edu.au/au/journals/PLPR/2000/45.html and elsewhere

[3] http://www.privacyconference2003.org/revents.asp

[4] http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html#RG

sont-ils proactifs dans leur rôle de réception des rapports d'ÉFVP? Se contentent-ils d'attendre les rapports, ou font-ils un suivi auprès des évaluateurs? Que devraient-ils faire?

- S'ils ont l'occasion de commenter un rapport, comment cela se passe-t-il? Ce processus exige-t-il beaucoup de ressources? Est-il approfondi?
- À quels problèmes doivent-ils faire face dans ces rôles?
- Quelles compétences faut-il pour effectuer ce genre de travail?
- Devraient-ils jouer d'autres rôles?
- Quelles sont les priorités des organismes de réglementation à ce stade?
- Quelle mesure réglementaire contribue le plus au succès des évaluations?
- Les organismes de réglementation font-ils la meilleure utilisation possible des rapports d'ÉFVP qu'ils reçoivent? Si la réponse est non, pourquoi, et que peut-on faire?
- Les organismes de réglementation travaillent-ils de façon transparente? Ces organismes ou les organisations évaluées mettent-ils les rapports des ÉFVP à la disposition des collectivités touchées ou de ceux qui gèrent la protection de la vie privée?

Partie D : La valeur

Les autorités de protection des données sont des organismes de réglementation polyvalents qui détiennent de nombreux pouvoirs et ont accès à de nombreux outils. Ces organismes utilisent-ils les ÉFVP correctement, et pour les bons projets? D'autres outils sont-ils parfois plus utiles? Les ÉFVP changent-elles quelque chose aux résultats concernant la vie privée? Comment le savons-nous?

Dans nos tentatives pour systématiser la gestion de la protection de la vie privée au moyen de l'ÉFVP et de systèmes semblables, ne serions-nous pas en train de « décerveler » le processus jusqu'à un point où il cesse d'être utile? Roger Clarke a-t-il raison de faire les remarques suivantes :

[traduction]

À partir de la fin des années 1990, les ÉFVP ont été reconnues par une succession d'organismes gouvernementaux comme une idée dont le temps était venu. On a préparé un grand

nombre de lignes directrices, avec des niveaux variables d'autorité et d'influence. Il est normal que la systématisation des procédures produise des procédures et des documents plutôt vides de sens. Un grand nombre de lignes directrices sont de la nature des listes de contrôle, et peuvent facilement conduire à la production de documents conformes aux lignes directrices. D'autres lignes directrices, cependant, sont intentionnellement conçues comme des introductions et visent à susciter des approches constructives à des problèmes généralement complexes et multidimensionnels.
Roger Clarke, *A History of Privacy Impact Assessments*, 2004[4]

Avons-nous des leçons à apprendre d'autres domaines des activités réglementaires, dans le secteur de la protection des données et ailleurs, qui pourraient nous indiquer comment mieux évaluer et en tirer des avantages pour la collectivité et la vie privée?

Questions pour alimenter la discussion :

- Que font actuellement les organismes de réglementation pour que les ÉFVP soient réellement profitables?
- Comment peut-on mesurer ou vérifier les résultats?
- Que pouvons-nous faire de plus, individuellement ou collectivement?
- D'après votre expérience, quelle mesure réglementaire contribue le plus au succès des évaluations?

Notes en bas de page

[1] http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html#Conc

[2] David Flaherty, "Privacy Impact Assessments: An essential tool for data protection", 2000, publié sur le site http://www2.garanteprivacy.it/garante/prewiew/0,1724,1619,00.html?sezione=116&LANG=1, sur le site http://beta.austlii.edu.au/au/journals/PLPR/2000/45.html et ailleurs.

[3] http://www.privacyconference2003.org/revents.asp

[4] http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html#RG

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Les évaluations des facteurs relatifs à la vie privée : de la théorie à la pratique

Getting Through Privacy Impact Assessments

Par/by:

Nigel Waters

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

L'animateur a soulevé les questions suivantes pour cette partie de l'atelier :

> « Une ÉFVP du modèle général utilisé dans cet atelier est réalisée non par l'organisme de réglementation, mais par une autre personne ou une autre équipe, généralement subordonnée à l'organisation dont le projet est soumis à l'évaluation. Dans ce contexte, l'organisme de réglementation a-t-il un rôle à jouer et, si oui, lequel? Est-il utile qu'il ait des contacts avec un évaluateur, ou bien cela a-t-il un effet sur l'indépendance de la relation entre l'évaluateur et l'organisme de réglementation? Les contacts dans l'intervalle peuvent-ils avoir pour effet que l'organisme de réglementation soit assailli de demandes de conseils ou d'opinions ponctuelles alors que l'objectif de l'ÉFVP est d'effectuer une évaluation systématique et scientifique des facteurs relatifs à la vie privée? Par ailleurs, si l'organisme de réglementation ne joue aucun rôle durant l'évaluation, cela va-t-il repousser les problèmes jusqu'à ce qu'il soit trop tard pour que l'organisme influe sur les événements? »

Dans cet atelier, on prend pour postulat que l'organisme de réglementation n'est pas nécessairement un commissaire à la protection des données ou de la vie privée, mais peut être un organisme externe dont le rôle est plus généralement de protéger les consommateurs ou de réglementer un secteur, ou encore un mécanisme de surveillance interne au sein d'une grosse bureaucratie.

Mon point de vue sur les problèmes que pose la relation entre l'organisme de réglementation et l'évaluateur vient de l'idée que le principal objectif d'une évaluation des facteurs relatifs à la vie privée (ÉFVP) est de servir l'intérêt public en cernant clairement l'incidence d'un projet sur la vie privée, en plus de proposer des manières de minimiser les répercussions dommageables sur la vie privée. De toute évidence, ce n'est pas toujours là l'objectif de l'organisation cliente, de l'organisme de réglementation ou de l'évaluateur s'ils voient leur rôle comme étant celui d'un consultant traditionnel. Dans la plupart des pays ou territoires administratifs, la *realpolitik* de la protection de la vie privée veut que les ÉFVP soient souvent commandées dans le but

The workshop leader has posed the following questions for this part of the workshop:

> "Privacy impact assessment on the typical model assumed in this workshop is performed not by the regulator but by another person or team typically answering to the organisation whose project is being assessed. So what if any role does or should a regulator play? Is it useful to be in touch with an assessor or does this affect the arms length relationship of assessor and regulator? Can contact lead to burdens being thrown onto the regulator who might be asked for *ad hoc* advice or opinions, whereas the purpose of PIA is to make the assessment of privacy impacts more systematic and scientific? On the other hand, does the regulator wish to hear about the direction an assessment is taken only when that assessment is over and it is too late to influence events?"

The premise of the workshop is that the regulator may not be a dedicated privacy or data protection Commissioner, but may be either an external agency with a more general consumer protection or sectoral regulatory role, or even an internal oversight mechanism within a large bureaucracy.

My views as to the issues that arise in relation to the regulator-assessor relationship are based on an assumption that the objective of a PIA is the public interest in clearly identifying all the privacy implications of a project, and in suggesting ways of minimizing adverse privacy impacts. This is not of course always the objective either of the client organisation, of the regulator, or of the assessor, if they see themselves purely as a traditional consultant. The 'realpolitik' of privacy in most jurisdictions means that PIAs will often be commissioned in support of a policy decision already made, and to create an illusion of privacy interests being considered, without any genuine commitment to do so.

My experience of conducting PIAs in Australia, New Zealand and Hong Kong suggests that there is no single model for the relationship between assessor and regulator in the course of a PIA.

Much depends on the relative expertise of the assessor, and of the regulator, in relation to PIA. In many jurisdictions, some assessors are significantly more experienced than the staff of the regulator, while others, particularly in consulting

d'appuyer une décision stratégique déjà prise et de créer l'illusion qu'on tient compte des intérêts en matière de vie privée, sans qu'il y ait d'engagement réel à le faire.

Mon expérience des ÉFVP en Australie, en Nouvelle-Zélande et à Hong-Kong m'incite à dire qu'il n'y a pas qu'un seul modèle de relation entre l'évaluateur et l'organisme de réglementation dans le cadre d'une ÉFVP.

L'expertise relative de l'évaluateur et de l'organisme de réglementation en matière d'ÉFVP fait une grande différence. Dans de nombreux pays ou juridictions, certains évaluateurs sont beaucoup plus expérimentés que le personnel chargé de la réglementation. Dans d'autres, surtout dans le cas de consultants qui se lancent tout juste sur le marché de la protection de la vie privée, les évaluateurs ne sont pas aussi familiers avec ce marché et bénéficieront des conseils de l'organisme de réglementation.

Par ailleurs, l'organisme de réglementation est également un intervenant clé et, c'est à espérer, un des principaux consommateurs de rapports d'ÉFVP[1]. Un évaluateur consciencieux doit tenir compte des points de vue de l'organisme de réglementation. Pour ce faire, il peut procéder à une consultation directe (si les consultations avec les intervenants font partie de la documentation de l'ÉFVP) ou il peut reconstruire le point de vue de l'organisme de réglementation d'après les commentaires et les opinions publiés ou d'après ses connaissances et son expérience.

Tant que l'ÉFVP sera nouvelle et relativement méconnue, la plupart des clients auront de la difficulté à comprendre la nature et les objectifs de celle-ci. De prime abord, on aura l'impression qu'il s'agit seulement d'une autre entreprise de consultation où le consultant a pour tâche de présenter le projet du client sous le jour le plus favorable possible pour ce qui est de ses incidences sur la vie privée. S'il a du mal à obtenir la coopération de son client ou à lui faire comprendre qu'il doit agir en tant qu'expert indépendant, l'évaluateur peut appeler l'organisme de réglementation afin d'obtenir son assistance.

À mesure que la technique d'ÉFVP deviendra courante, l'équilibre des rôles changera. De plus en plus d'évaluateurs seront des consultants « réguliers » dont la tâche sera d'aider les clients

businesses only just entering the privacy market, will not be as familiar and will benefit more from guidance from the regulator.

The regulator is also a key stakeholder, and also, hopefully, a main consumer of the PIA report[1], and a thorough assessor will ensure that the views of the regulator are taken into account. This may be by direct consultation (if stakeholder consultation forms part of the PIA brief) or by the assessor imputing a perspective to the regulator based on published views or comments or on knowledge and experience.

Most PIA clients, at least while the technique is still novel and unfamiliar, will have difficulty understanding the nature and objectives of a PIA. There will commonly be an expectation that it is just another consultancy engagement, in which the consultant's task is to present the client's project in the most favourable light, in terms of its privacy implications. An assessor facing difficulty in gaining either cooperation or understanding in the client agency in performing the desirable role of independent expert may find it useful to call the regulator 'in aid'.

As the PIA technique matures, the balance of roles may start to change. More assessors will be 'mainstream' consultants, with an initial presumption that their task is to assist the client in overcoming privacy 'hurdles', rather than making a neutral and dispassionate assessment. But in the same timeframe, regulators will hopefully have become more experienced in using third party PIAs to achieve their overall objective of ensuring a greater respect for privacy. Assuming an acknowledgement that this means more than just ensuring compliance with privacy requirements, but also dealing with stakeholder perceptions[2], the regulator may seek to become more involved in the progress of PIAs, to steer them in the right direction.

The relationship between regulator and assessor will of course depend partly on the relationship between the regulator and the client. Where the PIA has been imposed on the client organisation, either by the regulator or by some external requirement, there may be some reluctance to allow the assessor to have much contact with the regulator. Where there is a more co-operative starting point, such as where the client organisation has itself initiated the PIA and sees it as a helpful risk management tool, then there is

à régler des problèmes en matière de vie privée, plutôt que de faire des évaluations neutres et non biaisées. Parallèlement, les organismes de réglementation apprendront, du moins c'est à espérer, à utiliser les ÉFVP de tiers pour servir leurs propres objectifs de respect de la vie privée. Si on reconnaît que cela va plus loin que de simplement veiller au respect des exigences de préservation de la vie privée et si on comprend la nécessité de faire face aux perceptions des intervenants[2], l'organisme de réglementation peut chercher à participer davantage à l'élaboration de l'ÉFVP, afin de l'orienter dans la bonne direction.

Bien entendu, la relation entre l'organisme de réglementation et l'évaluateur dépendra en partie de la relation entre l'organisme de réglementation et le client. Si l'ÉFVP est imposée à l'organisation cliente par l'organisme de réglementation ou par une exigence externe, l'organisation peut se montrer réticente à l'idée de contacts trop soutenus entre l'évaluateur et l'organisme de réglementation. Si l'organisation cliente coopère depuis le début (si elle initie elle-même l'ÉFVP et la perçoit comme un outil de gestion des risques utile, par exemple), il est plus probable qu'elle permettra les échanges entre l'évaluateur et l'organisme de réglementation.

Une relation de collaboration *trop* étroite entre l'évaluateur et l'organisme de réglementation comporte cependant des risques. Si l'évaluateur est influencé outre mesure par les opinions et les idées préconçues de l'organisme de réglementation au sujet des enjeux pertinents, il pourrait perdre de vue d'autres éléments importants de la protection de la vie privée. On ne peut pas présumer que les organismes de réglementation sont obligatoirement à l'avant-garde du débat sur la vie privée ou qu'ils sont attentifs aux enjeux spécifiques que posent des projets précis. Un évaluateur expérimenté aura parfois pour tâche « d'aider l'organisme à rester honnête » en définissant les enjeux qui, en raison des politiques et des ressources, ne sont pas soulignés ou accueillis favorablement par l'organisme de réglementation. Dans d'autres situations où un organisme de réglementation expérimenté semble diriger un évaluateur inexpérimenté dans une direction précise, l'organisation cliente risque d'être sur la défensive et moins ouverte aux conseils de l'évaluateur que si ce dernier travaille clairement de manière indépendante.

likely to be a greater willingness to allow close contact.

There are risks in *too* close a relationship between a PIA assessor and the regulator. If the assessor is unduly influenced by the regulator's pre-conceptions of the relevant issues, other significant privacy impacts may be neglected. It cannot be assumed that regulators will necessarily be at the forefront of the privacy debate. Or sensitive to the particular issues arising in relation to specific projects. An experienced assessor will sometimes serve to 'keep the regulator honest' by identifying issues which, for political or resource reasons, the regulator has not highlighted, and may not necessarily welcome. But in other situations, where an experience regulator is seen to be steering an inexperienced assessor in a particular direction, the client organisation may be become defensive and less willing to take on boar the assessor's advice than if it is clear that they are independent of the regulator.

All of the discussion above has assumed that the relationship will be at the discretion of the client and/or assessor. Another possibility is that a particular relationship may be mandated, either directly by legislation, or by the regulator exercising powers under legislation. This may be considered necessary for 'quality control', and could for instance take the form of a requirement to submit a detailed project outline, or draft reports, to the regulator for review and comment during the course of a PIA. While no jurisdiction has gone this far, to my knowledge, it remains an option if, for instance, there was insufficient confidence in the ability of an unsupervised system to deliver quality PIAs.

As already noted, there is a risk that the introduction of the PIA technique, like the passage of privacy laws or the appointment of privacy regulators, could simply provide an illusion that privacy protection is being taken seriously, while in reality simply legitimising or 'rubber stamping' privacy intrusive developments. A useful analogy here may be the history of environmental impact assessment – many observers would suggest that while EIAs can sometimes make a valuable contribution to debate about the desirability of physical developments, they are all too often commissioned, designed and performed to support the approval of the development in question.

Les commentaires ci-dessus sont fondés sur la présomption que la nature de la relation sera entièrement à la discrétion du client ou de l'évaluateur. Une relation précise peut aussi être mandatée directement par la loi ou par un organisme de réglementation qui exerce ses pouvoirs en vertu d'une loi. On peut considérer cela nécessaire pour faire le « contrôle de la qualité ». Ainsi, l'évaluateur pourrait être tenu de soumettre un plan de projet détaillé ou des ébauches de rapports à l'organisme pour qu'il contrôle et fasse des commentaires pendant l'ÉFVP. Si, à ma connaissance, aucun pays ou aucune juridiction n'est allé jusque là, il s'agit néanmoins d'une possibilité lorsque, par exemple, on doute de la capacité d'un système non supervisé de réaliser des ÉFVP de qualité.

Comme on l'a déjà souligné, l'introduction de la technique des ÉFVP – tout comme l'adoption de lois sur la vie privée ou la nomination d'organismes de protection de la vie privée – pourrait simplement donner l'illusion que la protection de la vie privée est prise au sérieux, alors qu'en réalité, on justifie ou on donne le feu vert à des activités portant atteinte à la vie privée. Cette situation est comparable à celle de l'histoire des évaluations des impacts sur l'environnement. De nombreux observateurs suggèrent que, même si ces évaluations contribuent parfois utilement aux débats sur l'acceptabilité de projets de construction ou d'aménagement, elles sont trop souvent commandées, conçues et réalisées dans le but d'appuyer l'approbation des projets en question.

Conclusion

Si nous envisageons sérieusement d'utiliser les ÉFVP en tant qu'outils de protection de la vie privée, nous devons tenir compte de la grande importance de la relation entre l'évaluateur et l'organisme de réglementation. Il n'y a aucun modèle privilégié pour cette relation. Il faut plutôt tenir compte de nombreux facteurs et aspects qui influencent la relation dans le cadre de chacune des ÉFVP. Idéalement, ces influences ne doivent pas être laissées au hasard une fois l'ÉFVP commencée. Elles doivent être incluses dans le mandat, lequel doit néanmoins conserver une certaine souplesse pour permettre l'adaptation en cours de route. Aussi, l'organisme de réglementation peut à l'occasion intervenir de manière utile pour assurer le contrôle de la qualité

Conclusion

If we are serious about the use of PIAs as a tool to assist in protecting privacy, then the relationship between the assessor and the regulator matters – a lot! There is no one single preferred model for the relationship – rather a number of factors and dimensions that need to be taken into account in determining the relationship for each PIA. Ideally, this determination should not be left until the PIA is under way, but built into the terms of reference, although some flexibility for subsequent 'fine tuning' is desirable. There may also be a useful role for regulators to intervene on an exceptional basis to ensure quality control and engender confidence that the PIA technique is working as it should.

Examples of PIAs – Australia, New Zealand and Hong Kong

Published PIAs

- **Australian Bureau of Statistics**: **Census Enhancement Proposal, *2005***
- **New Zealand Government authentication for e-government, *2003-04***
- **Australian Attorney-General's Department - AML-CTF law, *2006***

PIAs known to have been commissioned but not published – references available

- **Australian National E-Health Transition Authority** Privacy Blueprint – PIAs on Unique Health Identifiers http://www.nehta.gov.au/index.php?option=com_docman&Itemid=139
- **Queensland Dept of Transport**: 'Smart' Drivers Licence, 2003
- **Australian Government** Access Card, 2006
- **Australian Government Information Management Office:** Identity management for Australian Government employees framework (IMAGE), 2006
- **Hong Kong Immigration Department** PIA for Hong Kong Smart Identity Card, 2000-01

Regulator Guides to PIA

Australian Privacy Commissioner, PIA Guide 2006 http://www.privacy.gov.au/publications/pia06/index.html

et promouvoir l'efficacité de l'ÉFVP.

Exemples d'ÉFVP – Australie, Nouvelle-Zélande et Hong-Kong

ÉFVP publiées

- **Bureau australien de la statistique :** Census Enhancement Proposal, 2005
- **Gouvernement de la Nouvelle-Zélande :** authentication for e-government, 2003-2004
- **Procureur général de l'Australie :** AML-CTF law, 2006

ÉFVP commandées mais non publiées – références disponibles :

- **Autorité nationale de transition à la santé électronique :** Privacy Blueprint – PIAs on Unique Health Identifiers http://www.nehta.gov.au/index.php?option=com_docman&Itemid=139
- **Ministère des transports de Queensland :** 'Smart' Drivers Licence, 2003
- **Gouvernement de l'Australie :** Access Card, 2006
- **Bureau de gestion de l'information du gouvernement de l'Australie :** Identity management for Australian Government employees framework (IMAGE), 2006
- **Ministère de l'immigration de Hong-Kong :** PIA for Hong Kong Smart Identity Card, 2000-2001

Guides pour les organismes de réglementation des ÉFVP

Commissaire à la protection de la vie privée de l'Australie, PIA Guide 2006
http://www.privacy.gov.au/publications/pia06/index.html

Commissaire à la protection de la vie privée de Victoria, PIA Guide 2004
http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf

Commissaire à la protection de la vie privée de la Nouvelle-Zélande, PIA Handbook, 2007
http://www.privacy.org.nz/library/privacy-impact-assessment-handbook

Victorian Privacy Commissioner, PIA Guide 2004
http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf

NZ Privacy Commissioner, PIA Handbook, 2007
http://www.privacy.org.nz/library/privacy-impact-assessment-handbook

Pacific Privacy July 2007

Endnotes

[1] Although all too often regulators seem to think they can leave a PIA to have the desired effect without follow-up. This will be the focus of another part of this workshop.

[2] This assumption should be discussed in other parts of the workshop, for instance in relation to setting the terms of reference and expectations.

Pacific Privacy, juillet 2007

Notes en bas de page

[1] Trop souvent, les organismes de réglementation semblent penser qu'une ÉFVP aura l'effet prévu, sans même qu'il y ait de suivi. On se penchera plus en détail sur cette question dans une autre partie de l'atelier.

[2] Ce postulat devrait faire l'objet d'autres discussions dans le cadre de l'atelier, par rapport à l'établissement des mandats et des attentes, par exemple.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Critères permettant d'établir la pertinence des évaluations des facteurs relatifs à la vie privée (ÉFVP) au Canada

Criteria for Evaluating the Adequacy of Privacy Impact Assessments (PIAs) in Canada

Par/by:

David H. Flaherty, Ph. D.

Juin 2007/June 2007

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Hypothèses du rédacteur

1. Les organisations doivent définir des critères applicables à l'évaluation de chaque ÉFVP qui tiennent compte des « pratiques exemplaires » adoptées par les experts en la matière.
2. Au moins plusieurs experts-conseils canadiens en protection des renseignements personnels, dont l'auteur du présent document, possèdent une expérience étendue de la réalisation des ÉFVP, particulièrement dans le domaine de la santé. Les organisations devraient envisager de recourir à leurs services pour les aider dans l'évaluation des ÉFVP qui leur sont soumises étant donné que la plupart des critères mentionnés ci-dessous nécessitent l'« œil d'un expert »; le chef de la protection des renseignements personnels d'une organisation pourrait parrainer cette activité au nom des parrains de projet de l'organisation.
3. En fait, les organisations pourraient établir un Comité consultatif sur les ÉFVP ou un Comité d'examen des ÉFVP, présidé par le chef de la protection des renseignements personnels, qui évaluerait toutes les ÉFVP qu'elles reçoivent. Le comité devrait comprendre des experts-conseils en protection des renseignements personnels et des représentants des utilisateurs (cliniciens, utilisateurs de technologies de l'information (TI), etc.) de divers systèmes d'information sur la santé, par exemple, dont la mise en œuvre est financée par une organisation.
4. Des extraits de ce qui suit proviennent de divers essais et documents rédigés par David Flaherty, y compris ses critiques à l'égard d'ÉFVP particulières effectuées par d'autres experts-conseils.

Liste de quelques critères d'évaluation pour les évaluations des facteurs relatifs à la vie privée

1. Traitement logique des sujets pertinents
2. Intégralité
3. Exactitude
4. Clarté
5. Bien-fondé juridique
6. Degré d'autorité
7. Gestion des risques d'atteinte à la vie privée
8. Perspective essentielle

Assumptions of the Drafter

1. An organization has to develop some criteria to apply to the evaluation of each PIA that reflect "best practices" followed by PIA experts.
2. There are at least several Canadian privacy consultants, including the present author, who have considerable experience with the execution of PIAs, especially in the health field. An organization should consider using them to assist in the evaluation of PIAs submitted to it since much of the criteria below require an "expert's eye"; an organization's Chief Privacy Officer could sponsor this activity on behalf of project sponsors at the organization.
3. In fact, an organization could set up a PIA Advisory Committee or a PIA Review Committee, chaired by the CPO, which would evaluate all PIAs that an organization receives. The committee should include some privacy experts/consultants, as well as user representatives (e.g. clinicians, IT users, etc.) of various health information systems, for example, whose implementation an organization is funding.
4. Portions of what follow come from various essays and work products of David Flaherty, including his critiques of specific PIAs prepared by other consultants.

A Listing of Some Evaluation Criteria for Privacy Impact Assessments

1. Logical Treatment of Relevant Topics
2. Comprehensiveness
3. Accuracy
4. Literateness
5. Legal Soundness
6. Authoritativeness
7. Managing Privacy Risk
8. Critical Perspective

1. Logical Treatment of Relevant Topics

- A standard PIA model is not essential, but there are topics that need to be included and treated in a PIA in a logical and sequential manner.[1] A basic narrative is almost always required in addition to tables, diagrams, and charts.
- In 2005, the consultant prepared a PIA model for the Ontario Smart Systems for Health Agency that measures for compliance with Ontario's *Personal Health Information Protec-*

1. Traitement logique des sujets pertinents

- Un modèle type d'ÉFVP n'est pas essentiel, mais certains sujets doivent être inclus et traités dans une ÉFVP de manière logique et séquentielle[1]. Un exposé sommaire est presque toujours requis en plus des tableaux, des diagrammes et des graphiques.
- En 2005, le consultant a élaboré un modèle d'ÉFVP pour l'Agence des systèmes intelligents pour la santé de l'Ontario qui mesure la conformité des organisations à la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario. Le document, qui comprend une importante série de questions sur chaque article pertinent de la Loi, couvre plus de cent pages. Il s'agit en fait d'un guide combiné sur la conformité et les ÉFVP. Aucune personne travaillant dans des dossiers électroniques de santé (DES) interopérables en Ontario, par exemple, ne manquera d'orientation sur la protection des données.
- Une ÉVFP doit mettre l'accent sur les questions hautement pertinentes liées à la protection des données qui se posent dans le cadre d'un projet particulier et prendre à leur égard une position éclairée et fondée sur des principes.
- L'ÉFVP ne devrait pas contenir de déclarations problématiques ou vagues qui, en fait, évitent de signaler les problèmes liés à la protection des données que l'ÉFVP doit analyser et résoudre.
- Une ÉFVP ne devrait pas accabler le lecteur en lui présentant des pages et des pages d'information brute, vague ou générale.

2. Intégralité

- Une ÉFVP devrait tenter d'éviter le concept d'une question ou d'un sujet « hors de portée » aux fins de l'évaluation et de l'atténuation des risques des questions liées à la protection des données dans une ÉFVP en particulier, à moins qu'il soit absolument nécessaire de le faire. (Il est tout à fait compréhensible que certaines questions soient « hors de portée », comme la future mise en place d'un système d'information, à propos duquel le fournisseur n'a peut-être pas de matériel écrit qu'il peut présenter aux clients). Mais dans certaines ÉFVP, il est déclaré – et ce, avec un plaisir apparent –

tion Act. It is a massive set of questions on every relevant section of the Act and runs to more than one hundred pages. It is in fact a combination compliance guide and PIA guide. No one working on interoperable EHRs in Ontario, for example, will lack for guidance on data protection.

- A PIA must focus on the highly relevant issues for data protection that arise in a particular project and take a principled, informed stand on them.
- The PIA should not contain problematic and/or vague statements that in fact avoid identifying problems for data protection that the PIA needs to analyze and resolve.
- A PIA should not overwhelm the reader with page after page of undigested, unfocused, and/or background information.

2. Comprehensiveness

- A PIA should try to avoid the concept of an issue or topic being "out of scope" for purposes of evaluating and mitigating data protection issues in a particular PIA, unless it is absolutely necessary to do so. (It is completely understandable that some issues are "out of scope," such as future releases of an information system, on which a vendor may not have any written materials that it can share with clients). But some PIAs take seeming delight in declaring that the tough issues for data protection are 'out of scope.'
- A PIA should ultimately address a project's compliance with each of the ten main privacy principles set out in the *Personal Information Protection and Electronic Documents Act* (PIPEDA), since it functions as the "national privacy standard" and the same principles can be found in equivalent provincial and territorial privacy (and health privacy) legislation.
- Where appropriate, a PIA should respond to the kinds of issues required to be examined in the "PIA models" that exist for jurisdictions like the federal government, Ontario, British Columbia, and Alberta. A project from a particular province has to take account of the local model in the conduct of a PIA.
- The core of an effective PIA is a careful description of how an information system (or any application of technology to personal information), actually works. In effect, the PIA "tells the story" of the application: why it exists

que les questions difficiles liées à la protection des données sont « hors de portée ».

- Une ÉFVP devrait essentiellement examiner la conformité d'un projet à chacun des dix principes clés de protection de la vie privée énoncés dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ), puisqu'elle tient lieu de « norme nationale en matière de protection de la vie privée » et les mêmes principes figurent dans les lois provinciales et territoriales équivalentes sur la protection de la vie privée (et la protection des renseignements personnels sur la santé).
- Au besoin, une ÉFVP devrait tenir compte des types de questions qui doivent être examinées dans les « modèles d'ÉFVP » qui existent dans les juridictions comme le gouvernement fédéral, l'Ontario, la Colombie-Britannique et l'Alberta. Un projet d'une province en particulier doit tenir compte du modèle local lors de la réalisation d'une ÉFVP.
- La base d'une ÉFVP efficace est une description minutieuse du fonctionnement d'un système d'information (ou de toute application de la technologie aux renseignements personnels). De fait, l'ÉFVP « raconte l'histoire » de l'application : pourquoi elle existe et comment elle recueille, utilise, communique et conserve les renseignements personnels. Dans ce processus, l'ÉFVP soulève des problèmes précis de protection de la vie privée et les résout de façon globale en se fondant sur une réflexion claire et des renseignements exacts. Il ne s'agit pas d'une tâche facile.
- Pour qu'une ÉFVP constitue un document de travail suffisamment crédible, elle doit contenir une description détaillée du contenu des principales sources de renseignements personnels dans tout système ou projet. Il n'est pas nécessaire que la description soit exhaustive, mais elle devrait donner aux lecteurs une bonne idée de la quantité, de la portée et du caractère identifiable des renseignements personnels que renferme le système. Cette description devrait également être axée sur la protection de la vie privée. L'un des buts principaux est de déterminer la mesure dans laquelle des renseignements personnels permettant l'identification se retrouvent dans une base de données, la mesure dans laquelle les renseignements ont été anonymisés de façon significative et les

and how it collects, uses, discloses, and retains personal information. In this process, the PIA surfaces and resolves specific privacy issues in a comprehensive manner on the basis of clear thinking and accurate information. This is not an easy task.

- To have sufficient credibility as a working document, a PIA should contain a detailed description of the contents of the main sources of personal information in any system or project. This does not have to be exhaustive, but it should provide readers with an appropriate sense of the amount, scope, and identifiablity of the personal information in the system. This description should also be privacy-focused. One major goal is to know the extent to which identifiable personal information exists in any data bases, the extent to which meaningful anonymization has occurred, and the risks of re-identification of any particular person, especially when record linkages, data mining, and data matching are possible or may be possible.
- A PIA must thus contain a detailed description of the personal information collected, used, disclosed, and retained for the proposed or existing project.
- A PIA should adequately address the issue of obtaining information consent for the personal information collected, used, disclosed, and retained for the proposed or existing project.
- A PIA should describe the overall privacy management framework at the relevant organization, health region, department or ministry and how the subject matter of the PIA will fit into it.[2]
- A PIA needs to draw out, and focus on, the implications for data protection of the key aspects of any particular proposed or existing project.
- A PIA should emphasize practices that have implications for data protection and surface the privacy issues. The sine qua non of an effective PIA is that it does the job of identifying these privacy risks, recommends concrete strategies for mitigating such risks, and seeks to resolve them.[3] Any PIA should accomplish this task in an effective and focused manner.
- A PIA should contain a coherent explanation of the disclosure avoidance practices for the project's use and disclosure of personal information.
- The PIA should also ensure that projects or

risques de ré-identification de toute personne en particulier, surtout lorsque le couplage de dossiers, l'exploration de données et le couplage de données sont possibles ou peuvent l'être.

- Par conséquent, une ÉFVP doit contenir une description détaillée des renseignements personnels recueillis, utilisés, communiqués et conservés pour le projet proposé ou existant.
- Une ÉFVP devrait adéquatement aborder la question de l'obtention du consentement pour les renseignements personnels recueillis, utilisés, communiqués et conservés pour le projet proposé ou existant.
- Une ÉFVP devrait décrire le cadre global de gestion de protection de la vie privée qui est propre à l'organisation, la région sanitaire, le département ou le ministère et la façon dont la matière traitée par l'ÉFVP s'y intégrera[2].
- Une ÉFVP doit dégager les répercussions, sur la protection des données, des principaux aspects de tout projet proposé ou existant, et être axée sur celles-ci.
- Une ÉFVP devrait mettre l'accent sur les pratiques qui ont une incidence sur la protection des données et souligner les problèmes de protection de la vie privée. Pour qu'une ÉFVP soit efficace, elle doit nécessairement cerner les risques d'atteinte à la vie privée, recommander des stratégies concrètes pour les atténuer et tenter de les résoudre[3]. Toute ÉFVP devrait accomplir cette tâche de manière précise et efficace.
- Une ÉFVP devrait contenir une explication cohérente des pratiques de protection de la vie privée concernant l'utilisation et la communication des renseignements personnels dans le cadre du projet.
- L'ÉFVP devrait également faire en sorte que les projets ou les systèmes qui utilisent de l'information anonyme ou pseudonyme définissent clairement de tels termes (pour s'assurer qu'ils utilisent effectivement de l'information « anonyme » ou « pseudonyme »).
- Pour aider les personnes concernées par les problèmes de protection de la vie privée mentionnés dans l'ÉFVP à mettre en œuvre diverses solutions de protection de la vie privée, l'ÉFVP devrait inclure un mécanisme permettant d'établir l'ordre de priorité des risques liés à la protection des données (p. ex. « risque faible », « risque moyen » ou

systems dealing with anonymous or pseudonymous information clearly define such terms (to ensure that they are in fact dealing with 'anonymous' or 'pseudonymous' information).

- To help the "owners" of the privacy problems identified in the PIA implement various privacy solutions, the PIA may want to include a mechanism for prioritizing data protection risks (e.g. "low risk", "medium risk," or "high risk") and associate these risks with particular timelines (e.g. implement solutions for "high risk" issues within 30 days, implement solutions for "medium risk" issues within 60 days, and implement solutions for "low risk" issues within 90 days).
- A PIA should conclude with a "privacy report card," in general, and for each of the ten privacy principles, as they are relevant to the subject matter of the PIA.
- The author(s) of a PIA should not segregate the reporting of relevant information from its analysis and from drawing conclusions. Issues should be dealt with as they arise in the PIA and be included in a summary overview or conclusion at the end. This being said, it is not unusual for some PIA readers (especially senior leadership) to scan the contents of a PIA fairly quickly. These individuals will want to see a succinct summary of privacy risks and recommendations for mitigating these risks in one, easy-to-find location in the PIA (usually the Executive Summary or a "summary of recommendations.")
- When identifying problems for data protection, a PIA should, to the fullest extent possible, present specific solutions as well.
- PIAs must be written with a critical eye to the sensitive issues of privacy and data protection, such as the risks of re-identification of individuals and the advancement of surveillance societies. The hard questions must be answered and "sales pitches" avoided, despite the obvious pressures to present a "clean" PIA to funders for approval. Organizations should, therefore, encourage funding recipients to be as frank and open as possible about potential privacy pitfalls associated with the systems or projects that are the subjects of its required PIAs.

3. Accuracy

- The PIA has to reflect the actual plans for the

« risque élevé ») et fixer des échéances particulières pour chacun de ces risques (p. ex. mettre en œuvre des solutions pour les questions à « risque élevé » dans un délai de 30 jours, les questions à « risque moyen » dans un délai de 60 jours et les questions à « risque faible » dans un délai de 90 jours).

- Une ÉFVP devrait se terminer avec un « bulletin sur la protection des renseignements personnels », en général et pour chacun des dix principes de protection de la vie privée, car ces derniers ont un rapport direct avec l'objet de l'ÉFVP.
- Le ou les auteurs d'une ÉFVP ne devraient pas séparer la communication d'information pertinente de son analyse et de la formulation de conclusions. Les questions devraient être traitées dès qu'elles sont soulevées dans l'ÉFVP et être incluses dans un aperçu sommaire ou une conclusion à la fin. Cela étant dit, il n'est pas inhabituel pour certains lecteurs d'ÉFVP (particulièrement la haute direction) de parcourir le contenu d'une ÉFVP assez rapidement. Ces personnes voudront consulter un résumé des risques d'atteinte à la vie privée et les recommandations pour atténuer ces risques dans une section facile à trouver de l'ÉFVP (habituellement le sommaire ou un « résumé des recommandations »).
- Lorsqu'elle cerne des problèmes liés à la protection des données, une ÉFVP devrait également présenter, dans la mesure du possible, des solutions précises.
- Les ÉFVP doivent être rédigées en posant un œil critique sur les questions sensibles de protection de la vie privée et de protection des données, comme les risques de ré-identification des personnes et le développement des sociétés de surveillance. On doit répondre aux questions épineuses et éviter les « arguments de vente », malgré les pressions évidentes pour qu'une ÉFVP « sans réserve » soit présentée aux bailleurs de fonds aux fins d'approbation. Par conséquent, les organisations devraient encourager les bénéficiaires de fonds à être aussi francs et ouverts que possible à l'égard des pièges éventuels pour la protection de la vie privée qui sont associés aux systèmes ou aux projets faisant l'objet des ÉFVP.

proposed project.

- The PIA should be fully documented from the project planning materials, such as the project charter, the business plan, technical specifications, an RFP, information from system vendors on privacy and security system features, etc., so that users of the PIA will know the authority for the information presented and have this documented.
- The PIA should also be documented from interviews with key project personnel as required. PIA questionnaires are another potential source.
- The "final" version of the PIA should reflect feedback from those managing the particular project and from those who will have ultimate responsibility or accountability for managing privacy risks (e.g. an organization's Chief Privacy Officer, even if he or she is not directly involved in the implementation of the system or project).

4. Literateness

- The PIA should be written at a simple enough descriptive and analytical level, in English or French, that an interested layperson, or media representative, will be able to understand and follow the PIA when it is made public.
- Clear, concise language for the text of the PIA avoids technical jargon to the greatest extent possible and explains it when avoidance is not possible.
- The PIA should avoid the use of abbreviations and acronyms that are not in common usage, since they make the PIA product very difficult for the uninitiated to read and understand (even with a glossary included).
- Organizations should encourage their funding recipients to ask a simple question: "If this PIA were to be made available to any of the patients/persons about whom personal information in the system or project relates, would such patients/persons be able to understand the PIA?" A related question is whether they would experience privacy 'sticker shock'?

5. Legal Soundness

- The primary purpose of a PIA is to allow the organization building or operating a personal information system, in the public or private sectors, to decide whether it is in compliance

3. Exactitude

- L'ÉFVP doit tenir compte des plans réels associés au projet proposé.
- L'ÉFVP devrait s'appuyer pleinement sur les documents de planification du projet, comme le mandat du projet, le plan d'activités, les spécifications techniques, la demande de proposition, les renseignements soumis par les fournisseurs de systèmes sur les caractéristiques de sécurité et de protection de la vie privée, etc., afin que les utilisateurs de l'ÉFVP connaissent la source de l'information présentée et que cela soit documenté.
- L'ÉFVP devrait également s'appuyer sur des entrevues avec le personnel clé du projet, au besoin. Les questionnaires des ÉFVP sont une autre source potentielle.
- La version « finale » de l'ÉFVP devrait tenir compte des commentaires des gestionnaires du projet et de ceux à qui incombe la responsabilité ultime de la gestion des risques d'atteinte à la vie privée (p. ex. le chef de la protection des renseignements personnels d'une organisation, même s'il ou elle ne participe pas directement à la mise en œuvre du système ou du projet).

4. Clarté

- L'ÉFVP devrait être rédigée à un niveau descriptif et analytique assez simple, en anglais ou en français, de façon à ce que les non-initiés, ou les représentants des médias, puissent comprendre et suivre l'ÉFVP lorsque celle-ci sera rendue publique.
- On devrait utiliser un langage clair et concis pour le texte de l'ÉFVP, éviter le jargon technique le plus possible ou fournir des explications, le cas échéant.
- On devrait éviter d'utiliser des abréviations et des sigles qui ne sont pas d'usage commun, autrement le non-initié aura beaucoup de difficulté à lire et à comprendre (même lorsqu'un glossaire est inclus).
- Les organisations devraient encourager leurs bénéficiaires de fonds à se poser une question simple : « Si cette ÉFVP était accessible à l'un ou l'autre des patients/ personnes concernés(ées) par les renseignements personnels du système ou du projet, est-ce que ces patients/personnes

with relevant data protection legislation at any particular stage in time. Every Canadian jurisdiction now has such laws in place.

- An important secondary goal is to meet the privacy expectations of the public with respect to moral, ethical, and human rights considerations, such as avoiding excessive surveillance and function creep. A PIA should be about more than legal compliance, especially in those jurisdictions which may have "weaker" or no health data protection statutes to "worry about."
- The PIA must accurately represent the legal standards for data protection that must be met for a particular jurisdiction or set of jurisdictions.
- The PIA must describe that level of privacy oversight that the project will receive on an ongoing basis, whether from a Ministry of Health, a hospital, and/or the local "privacy commissioner."
- In cases where the Ministry or other external oversight body (e.g. "privacy commissioner" or ombudsperson) will not have oversight, the PIA should clearly explain what other level of privacy oversight the project will receive on an ongoing basis. For example, the project may be reviewed annually by an organization's Chief Privacy Officer, an internal privacy team, or an external consultant.
- If "jurisprudence" on data protection exists for a jurisdiction, such as decisions of the courts or the "privacy commissioner," the PIA should document and present them as they are relevant to the project under consideration.
- If contractual conditions exist for the collection, use, and disclosure of personal information, then they need to be analyzed in the PIA for their relevance and adequacy for the required level of data protection. Then attention needs to be given to how these standards are implemented and made meaningful in practice. The latter activity should be a fundamental goal of any PIA, including the issue of resourcing of oversight activities.
- Establishing the legal framework for ensuring data protection is one of the core components of a successful PIA. Of course, the legal framework should be laid out for lay persons and not turned into a legal treatise (except in very rare, unusual circumstances).
- "Solutions" to such issues as applicable law and achieving information consent, for

pourraient comprendre l'ÉFVP? » Une question connexe serait la suivante : éprouveraient-ils un « choc » en ce qui concerne les questions de protection de la vie privée?

5. Bien-fondé juridique

- L'objectif principal d'une ÉFVP est de permettre à l'organisation qui instaure ou exploite un système de renseignements personnels dans les secteurs public ou privé de déterminer si toutes les étapes sont conformes aux lois sur la protection des données applicables. Chaque juridiction canadienne dispose maintenant d'une telle loi.
- Un objectif secondaire important est de répondre aux attentes du public en matière de protection des renseignements personnels sur le plan moral, éthique et des droits de la personne (p. ex., éviter la surveillance excessive et le détournement d'usage). Une ÉFVP ne doit pas uniquement examiner la conformité avec la loi, particulièrement au sein des juridictions qui ont un statut de protection des données sur la santé « plus faible », voire aucun.
- L'ÉFVP doit exposer de manière exacte les normes juridiques relatives à la protection des données qu'une juridiction ou un ensemble de juridictions doit respecter.
- L'ÉFVP doit décrire le niveau de surveillance de la protection des renseignements personnels que le projet recevra de manière continue, que ce soit de la part d'un ministère de la Santé, d'un hôpital ou du « commissaire local à la protection de la vie privée ».
- Dans les cas où le Ministère ou un autre organisme de surveillance externe (p. ex., un « commissaire à la protection de la vie privée » ou un ombudsman) n'assurerait pas la surveillance, l'ÉFVP devrait expliquer clairement quel autre niveau de surveillance de la protection des renseignements personnels le projet recevra de manière continue. Par exemple, le projet pourrait être vérifié annuellement par le responsable de la protection de la vie privée d'une organisation, une équipe interne chargée de la protection de la vie privée ou un expert-conseil.
- S'il existe dans une juridiction une « jurisprudence » sur la protection des données, comme les décisions d'un tribunal ou d'un « commissaire à la protection de la vie

example, will likely be transferable from one PIA to another, depending on the nature of the system or project, and if the thought processes of the team involved in preparing and revising the PIA are insightful and creative. Templates for such purposes can be transposed from one PIA to another. That has become the experience with PIAs at the Canadian Institute for Health Information.[4]

6. Authoritativeness

- A PIA should be authoritative and replicable in the sense that it can be updated to reflect changes in projects, data bases, or information systems. This requires detailed documentation of sources used in order to lend credibility to statements in the text of the PIA. Documentation should be to published materials, whenever possible. If draft materials are used, or more particularly interviews, these should also be documented in notes. The availability of credible documentation is a litmus test for the reliability of a PIA. But citation alone does not deliver the meaning and relevant analysis of whatever legal, or other, source is being quoted.
- The author(s) of a PIA have to adopt a consciously critical perspective in order to "dig below the surface to uncover the detailed realities of a system's or project's operations." The PIA should not be a promotional piece for a project. Thus it is inappropriate for the description of the scope of the PIA to include a statement like "… this PIA relies on information provided by the client and therefore does not constitute an audit of the client's privacy compliance mechanisms." This statement suggests an uncritical approach to the preparation of a PIA. A PIA is in effect a mini-audit of existing practices. Such a PIA needs to pose and to answer the relevant questions and to confirm the accuracy of information supplied to its drafters.
- An organization should not be "accepting" any PIA that does not cast an opinion on the project's attendant privacy risks and the organization's ability/willingness to implement specific risk mitigation strategies, especially for "high" privacy risks.

7. Managing Privacy Risk

- A PIA for a project is a major exercise in

privée », l'ÉFVP devrait la documenter et la présenter puisqu'elle est pertinente au projet à l'étude.

- S'il existe des dispositions contractuelles relatives à la collecte, à l'utilisation et à la communication de renseignements personnels, elles doivent être analysées dans le cadre de l'ÉFVP pour déterminer leur pertinence et leur justesse selon le niveau de protection des données requis. On doit ensuite prêter attention à la façon dont ces normes sont mises en œuvre et à la façon dont elles se concrétisent en pratique. Cette dernière activité devrait faire partie des objectifs fondamentaux de toute ÉFVP, notamment dans le cadre des ressources liées aux activités de surveillance.
- Un des éléments clés d'une bonne ÉFVP est l'établissement d'un cadre juridique pour garantir la protection des données. Évidemment, le cadre juridique doit s'adresser aux non-initiés et ne doit pas prendre la forme d'un traité (sauf dans des circonstances très rares et exceptionnelles).
- Les « solutions » à certains problèmes, comme les lois applicables et l'obtention du consentement à la communication d'information, pourront probablement être transférées d'une ÉFVP à l'autre selon la nature du système ou du projet et si l'équipe chargée de l'élaboration et de la révision de l'ÉFVP a des idées éclairées et novatrices. Un gabarit pourrait donc être utilisé pour toutes les ÉFVP. C'est ce qui se passe avec les ÉFVP de l'Institut canadien d'information sur la santé[4].

6. Degré d'autorité

- Une ÉFVP devrait faire autorité et pouvoir être reproduite; on pourrait ainsi la mettre à jour selon les changements apportés aux projets, aux bases de données et aux systèmes d'information. Cela exige la documentation détaillée des sources utilisées afin de garantir la crédibilité des déclarations énoncées dans l'ÉFVP. Le matériel cité dans la documentation devrait être publié, dans la mesure du possible. Si des ébauches ou, plus particulièrement, des entrevues sont utilisées, celles-ci devraient être également documentées sous forme de notes. La disponibilité de documents crédibles permet de déterminer la fiabilité d'une ÉFVP.

consciousness-raising about all aspects of data protection for any organization in the public or private sectors. It is also a way to anticipate and avoid privacy crises and privacy disasters.

- On the basis of a PIA, senior management can learn the exact issues that require decision-making on its part, especially with respect to privacy risk management.[5]
- Preparation of a PIA is usually impressive evidence of an organization's due diligence with respect to meeting data protection requirements for a particular project. Privacy and data protection, in this sense, are manageable issues.
- A secondary purpose of a PIA is to serve as an educational and negotiating tool for the system operators to use for purposes of compliance reviews by senior management and by the external data protection agent or agency. The PIA should make it relatively easy for executives and the privacy commissioner, and his or her staff, to understand how the system works and what the privacy issues and risks are. This argues for a sophisticated, narrative approach to the contents of a PIA that delivers all of the necessary details and does not skim over real issues; a narrative approach is also easier for a "layperson" to follow, such as a patient/person.
- The completion of an effective and meaningful PIA also requires a dialogue between the regulator and the regulated. Even more basically, it requires a dialogue between the person(s) drafting the PIA and the proponents of a system or project. This is an iterative process during the life of an information system.

8. Critical Perspective

- A basic function of a PIA is to ask probing, detailed questions of the proponents, builders, and designers of a project in order to promote comprehension. The role is in effect that of a devil's advocate for privacy.
- Organizations must prepare privacy-impact assessments in such a manner as to identify key problems, not gloss over them, or skip by them, since the health and IT specialists in the offices of "privacy commissioners" will focus on the "problem areas" in the long term.
- Internal advocates of innovative projects are naturally reluctant to be too critical of their

Cependant, une citation ne permet pas en elle-même de saisir le sens et d'analyser de manière pertinente les sources juridiques ou autres citées.

- Le(s) auteur(s) d'une ÉFVP doivent avoir un point de vue critique et consciencieux afin de creuser pour découvrir la réalité concernant les activités d'un système ou d'un projet. L'ÉFVP ne doit pas être considérée comme une activité faisant la promotion d'un projet. Il est donc inapproprié d'inclure dans la description de la portée de l'ÉFVP une déclaration comme celle-ci : « La présente ÉFVP est fondée sur les renseignements fournis par le client et ne constitue donc pas une vérification de ses mécanismes de protection des renseignements personnels. » Cette déclaration suppose une approche non critique à la préparation d'une ÉFVP. En fait, une ÉFVP constitue une mini-vérification des pratiques en place. Elle doit donc poser les questions pertinentes et y répondre et confirmer l'exactitude des renseignements fournis aux rédacteurs.
- Une organisation ne devrait pas « accepter » d'ÉVFP qui ne donne pas d'opinion sur les risques liés à la protection des renseignements personnels d'un projet ainsi que sur la capacité et la volonté d'une organisation de mettre en œuvre des stratégies précises d'atténuation des risques, particulièrement lorsqu'il s'agit de risques « élevés » liés à la protection des renseignements personnels.

7. Gestion des risques d'atteinte à la vie privée

- L'ÉFVP d'un projet est un exercice clé de sensibilisation à tous les aspects de la protection des données à l'intention de toute organisation du secteur public ou du secteur privé. Elle permet également de prévoir et d'éviter les crises et les catastrophes relatives à la protection des renseignements personnels.
- Grâce à une ÉVFP, la haute direction peut connaître les enjeux exacts à l'égard desquels elle doit prendre des décisions, particulièrement au chapitre de la gestion des risques liés à la protection des renseignements personnels[5].
- La préparation d'une ÉFVP est habituellement une preuve éloquente de la diligence

scheme. The best protection for such a project is for the difficult data protection questions to be posed and then resolved by presenting appropriate solutions as required. The process of resolution of issues is always incremental in character with senior management deciding levels of risk that they are willing to run and appropriate levels of investment in data protection and security.

Endnotes

[1] For an example of such headings in a model table of contents for a PIA, see David H. Flaherty, "Privacy Impact Assessments: An Essential Tool for Data Protection," in Stephanie Perrin, Heather H. Black, David H. Flaherty, and T. Murray Rankin, The Personal Information Protection and Electronic Documents Act: An Annotated Guide (Irwin Law, Toronto, 2001), p. 267.

[2] For a detailed description of a privacy management plan for Ontario hospitals, see Ontario eHealth Council, Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals. A Report Prepared by the Ontario Hospital eHealth Council Privacy and Security Working Group (Ontario Hospital Association, July, 2003, ISBN 0-88621-307-X), chapters 4 to 8 passim. The author was the consultant to this Working Group and the principal author of this report.

[3] In an ideal world, a PIA would resolve privacy issues which it identifies, but it may be more realistic to say that it is simply responsible for identifying concrete risk mitigation strategies. Part of the role of the PIA Advisory Committee or Review Committee at a large organization would be to follow up on any PIA it receives to see whether risk mitigation strategies outlined in the PIA were in fact ever adopted.

[4] See www.cihi.ca, 'privacy and data protection' link.

[5] The Ontario Management Board Guidelines state: "The end result of a privacy impact assessment process is documented assurance that all privacy issues have been appropriately identified and either adequately addressed or, in the case of outstanding privacy issues, brought forward to senior management for further direction." (p. 25)

raisonnable d'une organisation en ce qui concerne les exigences en matière de protection des données d'un projet spécifique. En ce sens, la protection des renseignements personnels et des données est une question gérable.

- Un autre objectif de l'ÉFVP est de servir d'outil éducatif et de négociation pour les gestionnaires de systèmes afin que la haute direction et l'agent ou l'agence externe de protection des données puissent procéder à un examen de la conformité. L'ÉFVP devrait aider la direction, le ou la commissaire à la protection de la vie privée et son personnel à comprendre le fonctionnement d'un système et à connaître les problèmes et les risques pour la protection de la vie privée qui en découlent.. Cela sous-entend une approche subtile et narrative à l'égard du contenu d'une ÉFVP qui donne tous les détails nécessaires et aborde en profondeur les vraies questions; de plus, un « non-initié » (p. ex. un patient, un membre du grand public) aura plus de facilité à comprendre une approche narrative.
- Une ÉFVP efficace et significative doit se terminer par un dialogue entre l'organisme de réglementation et l'entité réglementée. Autrement dit, il doit y avoir un dialogue entre les rédacteurs de l'ÉFVP et les promoteurs d'un système ou d'un projet. Il s'agit d'un processus itératif dans la vie d'un système d'information.

8. Perspective essentielle

- Une des fonctions de base d'une ÉFVP est de poser des questions d'approfondissement détaillées sur les promoteurs, les constructeurs et les concepteurs d'un projet afin d'assurer la compréhension des enjeux. Ici, il s'agit de jouer le rôle de l'avocat du diable en faveur de la protection de la vie privée.
- Les organisations doivent préparer des évaluations des facteurs relatifs à la vie privée afin de cerner les problèmes clés, et non pas de les dissimuler ou de les escamoter, puisque les spécialistes en santé et en TI des bureaux des commissaires à la protection de la vie privée mettront, à long terme, l'accent sur les problèmes.
- Les responsables internes de projets novateurs hésitent naturellement à critiquer

leur travail. La meilleure protection pour un tel projet consiste à poser des questions difficiles sur la protection des données et à les résoudre en présentant des solutions appropriées, au besoin. Le processus de résolution de problèmes va toujours de pair avec la détermination, par la haute direction, des niveaux de risque qu'elle accepte de tolérer et la mesure dans la quelle elle est prête à investir dans la protection des données et la sécurité.

Notes en bas de page

[1] Pour un exemple de titres du même genre dans une table des matières type pour une ÉFVP, voir David H. Flaherty, « Privacy Impact Assessments: An Essential Tool for Data Protection », et Stephanie Perrin, Heather H. Black, David H. Flaherty, et T. Murray Rankin, The Personal Information Protection and Electronic Documents Act: An Annotated Guide (Irwin Law, Toronto, 2001), p. 267.

[2] Pour une description détaillée d'un plan de gestion des renseignements personnels pour les hôpitaux de l'Ontario, voir le document intitulé Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals. A Report Prepared by the Ontario Hospital eHealth Council Privacy and Security Working Group (Association des hôpitaux de l'Ontario, juillet 2003, ISBN 0-88621-307-X), chapitres 4 à 8 passim. L'auteur était le consultant de ce Groupe de travail et le principal auteur de ce rapport.

[3] Dans un monde idéal, une ÉFVP réglerait les problèmes de protection de la vie privée qu'elle cerne, mais il serait peut-être plus réaliste de dire qu'elle est simplement responsable de l'identification de stratégies concrètes d'atténuation des risques. Une partie du rôle du Comité consultatif sur les ÉFVP ou du Comité d'examen des ÉFVP d'une grande organisation serait d'assurer le suivi de toutes les ÉFVP reçues afin de vérifier si les stratégies d'atténuation des risques ont effectivement été adoptées.

[4] Consultez le site www.cihi.ca et cliquez sur le lien « Confidentialité et protection des données ».

[5] D'après les lignes directrices du Conseil de gestion de l'Ontario, le résultat final d'une évaluation des facteurs relatifs à la vie privée est la garantie documentée que toutes les questions relatives à la protection des renseignements personnels ont été cernées et résolues de

manière appropriée ou, lorsqu'il s'agit de problèmes en cours, présentées à la haute direction pour que celle-ci prenne une décision à cet égard.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Modèle pour les évaluations des facteurs relatifs à la vie privée

Privacy Impact Assessments Template

Département de la Sécurité intérieure des Etats-Unis

US Department of Homeland Security

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Évaluation des facteurs relatifs à la vie privée pour

<<INSÉRER LE NOM DU SYSTÈME>>

<<INSÉRER la date de parution>>

Personnes-ressources

<<INSÉRER le type de personne-ressource>>
<<INSÉRER le programme/l'organisme/le bureau>>
<<INSÉRER l'élément/la direction>>
<<INSÉRER le numéro de téléphone de la personne-ressource>>

Agent de réexamen

Hugo Teufel III
Chef de la protection des renseignements personnels
Département de la Sécurité intérieure
703-235-0780

Résumé

Le résumé devrait comporter au moins trois phrases, mais pas plus que quatre phrases, au besoin, et respecter les consignes suivantes :

- La première phrase devrait indiquer le nom de l'élément ou du système.
- La deuxième phrase devrait décrire brièvement le système et sa fonction.
- La troisième phrase devrait expliquer la raison pour laquelle on procède à une évaluation des facteurs relatifs à la vie privée.

<< INSÉRER le résumé ici >>

Vue d'ensemble

La vue d'ensemble est la partie la plus importante de l'évaluation des facteurs relatifs à la vie privée. Une vue d'ensemble approfondie et claire offre au lecteur le contexte nécessaire pour comprendre les réponses contenues dans l'évaluation des facteurs relatifs à la vie privée. La vue d'ensemble devrait contenir les éléments suivants :

- le nom du système et le nom de l'élément ou des éléments du département à qui appartient le système;
- l'objectif du programme, du système ou de la technologie et la façon dont cet objectif est lié à la mission de l'élément et du département;
- une description générale de l'information contenue dans le système;
- une description d'une opération type effectuée dans le système;
- tout échange d'information effectué par le programme ou le système;
- une description générale des modules et des sous-systèmes, le cas échéant, et leurs fonctions;
- une citation demandant à l'autorité légale la permission d'exploiter le programme ou le système.

<< INSÉRER l'introduction ici >>

Section 1.0 Qualification des renseignements

Les questions suivantes visent à définir la portée des renseignements demandés et/ou recueillis, ainsi que les raisons pour lesquelles ils ont été recueillis dans le cadre du programme, du système, du règlement ou de la technique en cours d'élaboration.

1.1 Quels sont les renseignements recueillis, utilisés, diffusés ou conservés dans le système?

<< INSÉRER la réponse ici >>

1.2 Quelles sont les sources des renseignements contenus dans le système?

<< INSÉRER la réponse ici >>

1.3 Pourquoi les renseignements sont-ils recueillis, utilisés, diffusés ou conservés?

<< INSÉRER la réponse ici >>

1.4 Comment les renseignements sont-ils recueillis?

<< INSÉRER la réponse ici >>

1.5 Comment procédera-t-on pour vérifier l'exactitude des renseignements?

<< INSÉRER la réponse ici >>

1.6 Quels sont, précisément, les arrangements, les autorisations légales et/ou les ententes qui ont régi la collecte des renseignements?

<< INSÉRER la réponse ici >>

1.7 Analyse des facteurs relatifs à la vie privée : selon la quantité et le type de données recueillies, exposer les risques relatifs à la vie privée qui ont été définis et la façon dont ils ont été atténués.

<< INSÉRER la réponse ici >>

Section 2.0 Utilisation des renseignements

Les questions suivantes visent à clairement délimiter l'utilisation des renseignements et l'exactitude des données utilisées.

2.1 Décrire les différentes utilisations des renseignements.

<< INSÉRER la réponse ici>>

2.2 Quels sont les types d'outils utilisés pour analyser les données, et quel type de données peuvent être produites?

<< INSÉRER la réponse ici>>

2.3 Si le système utilise des données commerciales ou des données accessibles au public, donnez-en les raisons et expliquez la manière dont ces données sont utilisées.

<< INSÉRER la réponse ici>>

2.4 Analyse des facteurs relatifs à la vie privée : Décrire tous les types de contrôles mis en place pour s'assurer que les renseignements sont traités conformément aux utilisations décrites ci-dessus.

<< INSÉRER la réponse ici>>

Section 3.0 Conservation

Les questions suivantes visent à établir la durée de conservation des renseignements après la collecte initiale.

3.1 Pendant combien de temps les renseignements sont-ils conservés?

<< INSÉRER la réponse ici>>

3.2 La période de conservation a-t-elle été approuvée par l'archiviste et par la National Archives and Records Administration (NARA)?

<< INSÉRER la réponse ici>>

3.3 Analyse des facteurs relatifs à la vie privée : Exposer les risques liés à la durée de conservation des données, ainsi que la façon dont ces risques sont atténués.

<< INSÉRER la réponse ici>>

Section 4.0 Échange et communication internes de renseignements

Les questions suivantes visent à définir la portée des échanges de renseignements au sein du département de la Sécurité intérieure.

4.1 Avec quelle(s) organisation(s) interne(s) les renseignements sont-ils échangés? Quels sont les renseignements échangés? Et à quelles fins sont-ils échangés?

<< INSÉRER la réponse ici>>

4.2 Comment les renseignements sont-ils transmis ou communiqués?

<< INSÉRER la réponse ici>>

4.3 Analyse des facteurs relatifs à la vie privée : Selon l'étendue de la communication interne des renseignements, exposer les risques relatifs à la vie privée qui sont liés à la communication de renseignements, et la manière dont ces risques ont été atténués.

<< INSÉRER la réponse ici>>

Section 5.0 Échange et communication externes de renseignements

Les questions suivantes visent à définir le contenu et la portée de la communication de renseignements, ainsi que les autorisations législatives liées à la communication de renseignements à l'extérieur du département de la Sécurité intérieure, incluant le gouvernement fédéral, l'État, le gouvernement local, ainsi que le secteur privé.

5.1 Avec quelle(s) organisation(s) externe(s) les renseignements sont-ils échangés? Quels sont les renseignements échangés? Et à quelles fins sont-ils échangés?

<< INSÉRER la réponse ici>>

5.2 La communication, à l'extérieur du département, de renseignements personnels permettant l'identification est-elle conforme à la collecte initiale de renseignements? Si oui, est-elle visée par une utilisation régulière dans une notification relative aux systèmes de tenue des dossiers? Si c'est le cas, prière de fournir une description. Le cas contraire, dans le cadre de quel mécanisme légal le programme ou le système est-il autorisé à communiquer, à l'extérieur du département de la Sécurité intérieure, les renseignements personnels permettant l'identification?

<< INSÉRER la réponse ici>>

5.3 Comment les renseignements sont-ils communiqués à l'extérieur du département, et quelles sont les mesures de sécurité prévues pour protéger leur transmission?

<< INSÉRER la réponse ici>>

5.4 Analyse des facteurs relatifs à la vie privée : Dans le cadre de l'échange extérieur de renseignements, expliquer les risques relatifs à la vie privée et la manière dont ils ont été atténués.

<< INSÉRER la réponse ici>>

Section 6.0 Avis

Les questions suivantes concernent les avis qui sont communiqués aux personnes relativement à la portée des renseignements recueillis, au droit de consentir à l'utilisation de ces renseignements, et au droit de refuser de fournir des renseignements.

6.1 La personne a-t-elle été avisée avant que ne soit effectuée la collecte de renseignements?

<< INSÉRER la réponse ici>>

6.2 La personne peut-elle ou a-t-elle le droit de refuser de fournir des renseignements?

<< INSÉRER la réponse ici>>

6.3 La personne a-t-elle le droit de consentir à des utilisations particulières des renseignements? Si oui, comment exerce-t-elle ce droit?

<< INSÉRER la réponse ici>>

6.4 Analyse des facteurs relatifs à la vie privée : décrire la manière dont les avis sont communiqués aux personnes, et la manière dont les risques associés au fait que les personnes ne sont pas informées de la collecte des renseignements sont atténués.

<< INSÉRER la réponse ici>>

Section 7.0 Accès, recours et correction

Les questions suivantes concernent la capacité d'une personne d'assurer l'exactitude des renseignements la concernant qui ont été recueillis.

7.1 Quelles sont les procédures qui permettent aux personnes d'accéder à leurs renseignements?

<< INSÉRER la réponse ici>>

7.2 Quelles sont les procédures permettant de corriger des renseignements inexacts ou erronés?

<< INSÉRER la réponse ici>>

7.3 Comment les personnes sont-elles avisées des procédures qui visent à corriger leurs renseignements?

<< INSÉRER la réponse ici>>

7.4 Si aucun recours officiel n'est fourni, quelles solutions de rechange sont offertes?

<< INSÉRER la réponse ici>>

7.5 Analyse des facteurs relatifs à la vie privée : Quels sont les risques relatifs à la vie privée associés aux recours offerts aux personnes? Comment ces risques sont-ils atténués?

<< INSÉRER la réponse ici>>

Section 8.0 Accès technique et sécurité

Les questions suivantes sont axées sur les dispositifs techniques de protection et les mesures de sécurité.

8.1 Quelles procédures ont été mises en place pour déterminer quels utilisateurs peuvent accéder au système? Ces procédures sont-elles documentées?

<< INSÉRER la réponse ici>>

8.2 Les entrepreneurs du département auront-ils accès au système?

<< INSÉRER la réponse ici>>

8.3 Décrire la formation fournie aux utilisateurs sur la protection de renseignements personnels et qui se rapporte essentiellement ou de façon générale au programme ou au système.

<< INSÉRER la réponse ici>>

8.4 Le système ou les systèmes appuyant le programme ont-ils été accrédités ou certifiés?

<<INSÉRER la réponse ici>>

8.5 Quelles sont les mesures de vérification et les mesures techniques de protection qui ont été mises en place pour prévenir le mauvais usage de données?

<<INSÉRER la réponse ici>>

8.6 Analyse des facteurs relatifs à la vie privée : Selon la sensibilité et la portée des renseignements recueillis, et dans l'éventualité de tout échange de renseignements effectué dans le système, quels sont les risques relatifs à la vie privée et comment les contrôles de sécurité permettent-ils de les atténuer?

<< INSÉRER la réponse ici>>

Section 9.0 Technologie

Les questions suivantes visent à analyser de façon critique le processus de sélection des technologies utilisées par le système, y compris le matériel, l'identification par radiofréquence, la biométrie et autres technologies.

9.1 À quel type de projet le programme ou le système est-il associé?

<< INSÉRER la réponse ici>>

9.2 À quelle étape de son élaboration le système est-il rendu? Quel processus a été choisi pour l'élaboration du projet?

<< INSÉRER la réponse ici>>

9.3 Dans le cadre du projet, utilise-t-on des technologies pouvant susciter des préoccupations en matière de protection de la vie privée? Si oui, commenter leur mise en œuvre.

<< INSÉRER la réponse ici>>

Page d'approbation et de signature

_____

Hugo Teufel III

Chef de la protection des renseignements personnels

Département de la Sécurité intérieure

Privacy Impact Assessment
for the

<<ADD SYSTEM NAME>>

<<ADD Publication Date>>

Contact Point
<<ADD Type Contact Person>>
<<ADD Program/Agency/Office>>
<<ADD Component/Directorate>>
<<ADD Contact Phone>>

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

<< ADD Abstract Here >>

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

<< ADD Introduction Here >>

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

<< ADD Answer Here >>

1.2 What are the sources of the information in the system?

<< ADD Answer Here >>

1.3 Why is the information being collected, used, disseminated, or maintained?

<< ADD Answer Here >>

1.4 How is the information collected?

<<ADD Answer Here>>

1.5 How will the information be checked for accuracy?

<< ADD Answer Here >>

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

<< ADD Answer Here >>

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

<< ADD Answer Here >>

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

<< ADD Answer Here >>

2.2 What types of tools are used to analyze data and what type of data may be produced?

<< ADD Answer Here >>

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

<< ADD Answer Here >>

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

<< ADD Answer Here >>

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

<< ADD Answer Here >>

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

<< ADD Answer Here >>

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

<< ADD Answer Here >>

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

<< ADD Answer Here >>

4.2 How is the information transmitted or disclosed?

<< ADD Answer Here >>

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

<< ADD Answer Here >>

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

<< ADD Answer Here >>

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

<< ADD Answer Here >>

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

<< ADD Answer Here >>

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

<< ADD Answer Here >>

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

<< ADD Answer Here >>

6.2 Do individuals have the opportunity and/or right to decline to provide information?

<< ADD Answer Here >>

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

<< ADD Answer Here >>

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

<< ADD Answer Here >>

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

<< ADD Answer Here >>

7.2 What are the procedures for correcting inaccurate or erroneous information?

<< ADD Answer Here >>

7.3 How are individuals notified of the procedures for correcting their information?

<< ADD Answer Here >>

7.4 If no formal redress is provided, what alternatives are available to the individual?

<< ADD Answer Here >>

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

<< ADD Answer Here >>

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

<< ADD Answer Here >>

8.2 Will Department contractors have access to the system?

<< ADD Answer Here >>

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

<< ADD Answer Here >>

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

<< ADD Answer Here >>

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

<< ADD Answer Here >>

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

<< ADD Answer Here >>

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

<< ADD Answer Here >>

9.2 What stage of development is the system in and what project development lifecycle was used?

<< ADD Answer Here >>

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

<< ADD Answer Here >>

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security