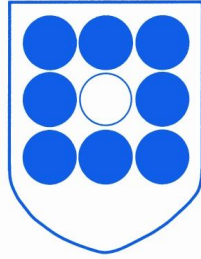


CANADIAN CIVIL LIBERTIES ASSOCIATION

360 Bloor Street West, Suite 506
Toronto, ON M5S 1X1
Telephone (416) 363-0321
Fax (416) 861-1291
E-mail: mail@ccla.org



ASSOCIATION CANADIENNE DES LIBERTES CIVILES

360 rue Bloor Ouest, Suite 506
Toronto, ON M5S 1X1
Téléphone (416) 363-0321
Télécopieur (416) 861-1291
Courriel: mail@ccla.org

EXECUTIVE COMMITTEE COMITÉ EXÉCUTIF

Past Presidents Présidents Précédents

J. KEILLER MACKAY
(1888-1970)
J.S. MIDANIK, Q.C.
(1920-1997)
JOHN NELLIGAN, Q.C.
HARRY W. ARTHURS
ALTER TARNOPOLSKY
(1932-1993)
WALTER PITMAN
SYBIL SHACK
(1911-2004)
DR. ALLAN BLAKENEY

President Présidente

MARSHA HANEN

Vice-presidents Vice-présidentes

JAMIE CAMERON
SUSAN COOPER
CÔTE-HARPER, Q.C.
MARLYS EDWARDH
L. GREENSPAN, Q.C.
PATRICIA JACKSON
JOHN D. McCAMUS
DELIA OPEKOKEW
DR. HOWARD PAWLEY
KENNETH P. SWAN
DR. JOSEPH WONG

Secretary Secrétaire

DNEY GOLDENBERG

Treasurer Trésorière

ELAINE SLATER

General Counsel Avocat Général

THALIE DES ROSIERS

BOARD OF DIRECTORS D'ADMINISTRATION

FRANK ADDARIO
RREN ALLMAND, Q.C.
ROMLEY ARMSTRONG
RONALD ATKEY, Q.C.
FREDERIC BACHAND
JOSEPH BOYDEN
EDWARD BRODBENT
LEAH CASSELMAN
SAUL CHERNIAK, Q.C.
DOMINIQUE CLÉMENT
JANE COBLEN
MICHAEL CONNER
DR. DEBBY COPES
DAVID CRONENBERG
FERNAND DAOUST
PETER DESBARATS
BRIAN A. F. EDY
SUSAN ENG
MEL FINKELSTEIN
ROBERT FULFORD
VICKI GABEREAU
ANCE R. GLUBE, Q.C.
KATHERINE GOVIER
LOUIS GREENSPAN
HUSSEIN HAMDANI
SHIRLEY HEAPEY
HARISH JAIN
MUHMUD JAMAL
JANET KEEPING
JOY KOGAWA
ANNE La FOREST
CYRIL LEVITT
ANDREW LOKAN
A. WAYNE MACKAY
KEN MANDZUIK
JON OLIVER
PENELOPE ROWE
PAUL SCHABAS
MARVIN SCHIFF
VID SCHNEIDERMAN
ERIC TEED, Q.C.
WALTER THOMPSON
Y REV. LOIS WILSON

ion & Administration ion et administration

D. S. McLAUGHLIN

of Expression Project Project de la liberté d'expression

A MENDELSON AVIV

Public Safety Project de sécurité publique

GRAEME NORTON

ral Counsel Emeritus ocat Général émérite

A. ALAN BOROVY

May 14, 2010

Gary K. McDonald
Director General
Legislation and International Relations Bureau
Passport Canada

BY EMAIL: consultations@pptc.gc.ca

Dear Mr. McDonald:

Thank you for your invitation to the CCLA to provide our written input on the introduction of biometric passports (also referred to as ePassports or electronic passports) in Canada. We provide our comments below.

Context

We understand that the proposed biometric passports will contain an "electronic chip" that will store:

1. Personal and private identifying information currently available on page 2 of each passport, i.e. surname, given names, date of birth, place of birth, gender;
2. A "digital picture" in jpeg format of the bearer's photograph on page 2, thereby employing the "facial recognition" biometric, as opposed to the iris or fingerprint biometrics; and
3. A country-specific signature to prove the passport is issued by Canada, which is verified through use of the Public Key Infrastructure (PKI).

The CCLA notes Passport Canada's rationale that ePassports are being introduced to enhance security, fight fraud, and reduce identity theft. We are aware that biometrics have been introduced internationally as a counter-terrorism measure, are already in use in the US, the EU, Australia, Israel, in travel documents. Passport Canada reports that 60 countries have introduced biometric passports worldwide, and that 25000 diplomatic and private ePassports have already been issued in Canada without 'incident'.

Obviously the goals of greater security and authenticity of passports are laudable, and to large extent the introduction of biometric passports is a *fait accompli*.

In this light, our comments revolve around concerns of accuracy and privacy of Canadian passport-holders. The CCLA believes new technologies such as biometric passports should be implemented with adequate legal safeguards. We are interested in knowing what measures Passport Canada has taken to-date and intends to take going forward, to ensure the civil liberties of Canadians including the rights of privacy and mobility, are been protected. Our specific questions and recommendations are set out below.

GENERAL PRIVACY CONCERNS AND THE CREATION OF DATABASES

The right to privacy enjoys constitutional protection under section 8 (the right to be free from unreasonable search and seizure) of the *Canadian Charter of Rights and Freedoms*, and is protected under the federal *Privacy Act*.

Privacy is also protected in international law, namely by Article 17 of the International Covenant on Civil and Political Rights, which has been ratified by Canada. Generally, the right to privacy in democratic nations is considered a fundamental tenet of a free and democratic society, and a cornerstone right from which the ability of an individual to enjoy other fundamental rights and liberties flows.

New information technologies generating personal data resulted in the development of core international privacy principles. These include, as identified by the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering terrorism¹:

- Obtaining personal information fairly and lawfully;
- Limiting the scope of use to the originally specified purpose;
- Ensure that processing is adequate, relevant and not excessive;
- Ensuring accuracy;
- Keeping data secure;
- Deleting data when no longer required; and
- Granting individuals the right to access their information and request corrections.

The above principles are generally in keeping with Canada's privacy protection schemes.²

However, not all countries comply with our privacy protection values. Further, in the counter-terrorism era in which we now live, even democratic States have at times relaxed their privacy protection safeguards, and non-democratic states with

¹ See Report to the Human Rights Council, Thirteenth Session, 28 December 2009, A/HRC/13/37 focusing generally on the right to privacy in the context of counter-terrorism, at paragraph 12.

² Generally, the Privacy Act for government use of personal information, and the PIPEDA for private sector use of personal information.

lesser privacy protection values have accessed private and personal information to demonstrably increase their surveillance powers.

Canadians traveling with biometric passports will be subject to the privacy practices of other states, including foreseeably the retention of the personal identifying information of Canadian citizens in foreign databases. The CCLA would like to know what considerations if any Passport Canada has taken of this inevitability? The CCLA is concerned that Passport Canada may be extending access (storage and retention) of the personal information of Canadian citizens to foreign governments and actors, without Canada's legal privacy safeguards or constitutional protections. While Canadian citizens understand they have restricted privacy rights at international borders, they are not necessarily consenting to the information contained on the RFID chip in the passport being stored in a foreign government's database.

Finally, the CCLA notes that the Order Amending the Canadian Passport Order provides that Passport Canada can convert information into use for biometric use or "any other uses that fall within the mandate of Passport Canada."³ The CCLA would like to know what "other uses" are contemplated by Passport Canada.

COMMENT 1: Please provide more information on what steps Passport Canada has taken, or will take – or what international safeguards currently exist that Passport Canada has considered – that apply privacy safeguards to limit retention in foreign databases of personal information of Canadians available on the RFID chip in the biometric passport.

Passport Canada has used digital photo images in passports since 2002. Biometric passports have been introduced since 2006, with as noted above, 25000 diplomatic and other biometric passports already issued. Commentators, and the Special Rapporteur considering this issue, have noted with concern "function creep" wherein information and data gathered for one purpose may be used surreptitiously and without consent, for other purposes.

COMMENT 2 (a): Please provide information on any database Passport Canada has created of the images and personal information of Canadian passport holders. Please provide information on how this information is being used, and what parties have access to this information, and any "other uses" of biometric information. Please inform us whether Canadians have the right to access their information and request changes as necessary.

COMMENT 2(b): Please confirm whether the information in the biometric passport will be used to compare Canadians to criminal watch-list or terrorist-suspect databases in Canada or abroad, and what control or safeguards if any Canada has over this process.

³ Order Amending the Canadian Passport Order, SI/2006-95, June 28, 2006, Canada Gazette, Vol. 140, No. 13, paragraph 6, replacing section 8 of the Canadian Passport Order.

COMMENT 3: We understand a Privacy Impact Assessment was done on the implementation of biometric passports and is available currently pursuant to an Access to Information Request. Please make the PIA publicly available, with comments as to how Passport Canada has addressed any concerns raised by the PIA.

FACIAL RECOGNITION BIOMETRICS

Biometrics do not just contain information about a person, but also “of the person”.⁴

Canada’s biometric passport will use facial recognition biometrics. Facial biometrics are the preferred biometric of the ICAO, with the option for States to combine this with iris or fingerprinting biometrics.⁵

The CCLA understands that the facial recognition biometric is considered to be the least intrusive biometric, because compared to iris recognition and fingerprinting, it does not require interaction by the individual with a physical device⁶, and discloses the least amount of information. Researchers report that iris scan and fingerprints each can disclose information relating to private health issues such as the presence of diabetes, hypertension, HIV, misuse of drugs and alcohol, and even homosexuality – all of which is personal private information that can be used against the individual.⁷ Another argument in favour of facial recognition is that people, generally, voluntarily expose their faces to the public.

The arguments against facial recognition as the primary biometric are as follows: it has the highest error rate; templates of facial biometrics can be created from a jpeg image but there is no international standardization of templates thus increasing the probability for false acceptance or false rejection; faces are in a

⁴ Anne-Marie Hayden, spokesperson for the Privacy Commissioner, stating “Biometrics can be used and misused. When properly handled, biometrics can offer strong authentication and can actually enhance individuals’ privacy and control of their own identity. Misused, of course, biometrics can lead to undesirable privacy invasions...Collecting biometric information about individuals raises obvious and significant privacy concerns. It engages bodily and informational aspects of privacy; it doesn’t just involve the collection of information about a person, but rather, information of the person. It’s really the ultimate in personal information,” as reported in The Toronto Star, “Ottawa takes “big step” to biometric ID: Proposed changes to affect passports, Privacy Czar vows to watch for abuses”, by Susan Delacourt, Ottawa Bureau Chief, (2006) available at <http://www.sulemanco.com/node/9>.

⁵ See generally ICAO Document 9303 governing biometrics.

⁶ Gerrit Hornung, “Biometric Identity Cards: Technical, Legal and Policy Issues,” in S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2004), 47-57 at p. 48.

⁷ Ibid.

constant state of change⁸; and facial biometrics open a Pandora's box for mass surveillance by States of individuals and a corresponding chilling effect on many civil liberties.

COMMENT #4: Please provide information on what measures Passport Canada will employ to address false acceptance and false rejection rates. Please provide information on what remedies or recourse will be available to individuals falsely identified, other than recourse under the Privacy Act.

COMMENT #5: Please provide information on what measures if any have been considered by Passport Canada regarding domestic or international use of the jpeg images. Please also see Comment #1 above.

SECURITY

Because of their ability to be read or scanned by third parties (public or private) without the knowledge of the bearer, it is important that RFID have in-built security features.⁹

CCLA understands from Passport Canada's description, that the RFID in the ePassport can only be read within 10 centimetres, and requires the passport to be open before the passport can be read. The choice to use a short-range proximity RFID is desirable. Still, the CCLA questions whether evolving technology will enable the surreptitious reading of Canadian passports in airports or other new frauds, i.e. "fraud shift". The CCLA has been informed that low-cost commercially available software already permits the reading of RFID chips in close proximity.¹⁰

The CCLA recommends that Passport Canada consider methods to prevent surreptitious reading of passports in close proximity. The CCLA has been informed that US passports are embedded with metal foil to add another layer of protection (i.e. still not impenetrable) against surreptitious reading of the RFID chip, and the proposed EDLs were to be distributed in a metal case. Has Passport Canada considered any such security measures?

COMMENT #6: The CCLA recommends the use of effective protective measures to guard against surreptitious reading or cloning of the RFID chip in close proximity, and request information on what measures Passport Canada may be considering.

⁸ Consider the 2009 case of Suaad Hagi Mohamud, a Canadian woman who was erroneously accused by Kenyan border officials of impersonation because they thought she did not look like her passport photo. Canadian consular officials concurred that she was an imposter and voided her passport. She was stranded in Kenya for three months before DNA evidence proved her identity.

⁹ EC 12.5.2009 paragraph (6).

¹⁰ Professor Andrew Clement, telephone conversation Tuesday May 11th, 2010.

CCLA welcomes Passport Canada's assurances that the passport chip is subject to the Public Key Infrastructure, wherein the border guard can use the public key to verify the digital signature indicating that the passport has been issued by Canada. Indeed, we are told that when all the security mechanisms are in place and being used, the possibility for fraud is dramatically reduced if not impossible. However, CCLA is informed that not all countries are checking digital signatures of biometric passports.

COMMENT #6: Please provide information on when the PKI infrastructure will be internationally implemented and any impediments to that goal.

We thank you for the opportunity to provide our written input on biometric passports.

We look forward to hearing from you on this matter.

Sincerely,

A handwritten signature in black ink, appearing to read 'N. Des Rosiers', with a long horizontal flourish extending to the right.

Nathalie Des Rosiers
General Counsel