An Open Letter to the ICAO

A second report on 'Towards an International Infrastructure for Surveillance of Movement'

Tuesday March 30, 2004

To the participants of the International Civil Aviation Organization 12th Session of the Facilitation Division,

We are writing to you on behalf of a wide range of human rights and civil liberties organizations to express our concerns regarding a number of decisions emerging from your conferences and their likely effects on privacy and civil liberties. We are particularly worried about your plans requiring passports and other travel documents to contain biometrics and remotely readable 'contact-less integrated circuits'.

We are increasingly concerned that the biometric travel document initiative is part and parcel of a larger surveillance infrastructure monitoring the movement of individuals globally that includes Passenger-Name Record transfers, API systems,[1] and the creation of an intergovernmental network of interoperable electronic data systems to facilitate access to each country's law enforcement and intelligence information.[2]

We are concerned that the ICAO is setting a surveillance standard for the rest of the world to follow. In this sense, the ICAO is setting domestic policy, implementing profiling and ID cards where previously none may have existed, or enhancing ID documentation through the use of biometrics, and increasing the data pouring into national databases, or creating them when none previously existed.

While we understand the desire of the ICAO to increase confidence in travel documents, reduce fraud, combat terrorism, and protect aviation security, the implementation of biometrics will have disproportionate effects on privacy and civil liberties. These rights are enshrined in a number of international conventions and treaties including article 12 of the United Nations Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and a number of national constitutions and legal systems. The actions of the ICAO threaten these rights.

Protecting the privacy of movement

Respecting the privacy of individuals is essential to an open society, including travel privacy. The right to movement is viewed as a fundamental right around the world, akin to the right to assemble. Border and aviation security necessarily involves scrutinising travellers and the use of personal information, but in light of the fundamental human rights involved, must be approached with the utmost thought and care. The ICAO's biometrics-based approach to securing travel documents unfortunately does not reflect such care – in fact, it is enabling the creation of a global surveillance infrastructure.

Concern about biometric travel documents is high around the world, and has been recognized even by many national governments:

- The U.S. Department of Homeland Security and the Department of State note that privacy issues need to be resolved prior to the implementation of these systems.[3]
- Even as the European Commission has advocated a centralised database solution, storing the biometrics of all EU travel document holders, it has noted that further research is necessary to "examine the impact of the establishment of such a European Register on the fundamental rights of European citizens, and in particular their right to data protection."[4]

- The French Government has concluded similarly, requiring that any implementation of biometric techniques is systematically subject to prior agreement from its national privacy commission.[5]
- As ICAO has itself noted, some States are legally barred from storing biometrics.[6]

Avoiding national biometric databases

Because they are not carefully crafted, the ICAO standards risk ignoring these international warnings, resulting in the creation of centralized national databases of personal biometric information.

The European Union, for example, is already using the call for biometric passports to propose the establishment a central European store of fingerprints, which would enable national databases, national-ID cards,[7] and background searches.[8] The EU is also calling for storage capacity on the chips contained in its passports to be significantly larger than the ICAO standard of 32K, thus allowing for additional information to be included in the future,[9] enabling further function creep.

Central databases become privacy risks through the disclosure of personal information, through the challenges of securing such large data stores, and through the use of biometric data for other purposes. Additionally, the centralised storage of biometric data increases the risk of the use of biometric data as a key to interconnecting databases that, according to EU privacy officials "could lead to detailed profiles of an individual's habits both in the public and in the private sector".[10]

Such databases will also lead to the increased transfer of personal information across borders as individuals travel. When an EU citizen's identity is verified in the U.S., for example, will the American authorities download the facial and fingerprint data from the EU databases, or will U.S. authorities retain the biometric data they collect when verifying the document, along with other similar data for the next 50 years? Similarly, when citizens of other countries visit EU member states, will they be required to submit fingerprints even though the ICAO travel documentation standards do not require fingerprint data? Until these questions are resolved, no standards for interoperability should be established at the ICAO.

Already there is some discussion of sharing biometric information with private companies. Airline check-in procedures will involve verifying the integrity of the travel documents, and airlines may retain the biometrics data. As part of the Advanced Passenger Information systems, some foresee the biometric information also being transferred by airlines to government agencies at passengers' destinations.[11]

Technologies in the Surveillance Infrastructure

Biometrics is a fallible technology that will increase surveillance, erroneously subject individuals to undue attention, and, unless implemented carefully, will lead to increased collection and processing of data and transfer across borders.

The ICAO's choice of facial recognition as the standard remains problematic:

- Facial recognition contains a high likelihood of false non-matches (where valid individuals are refused border entry because the technology fails to recognise them), and false matches (where an individual is matched to another individual incorrectly).[12] The ICAO standards do not govern the use to which the facial recognition data is put, but even the most reliable uses of this technology – one-to-one verification using recent photographs – have been shown in U.S. government tests to be highly unreliable, returning a false non-match rate of 5 percent and a false match rate of 1 percent.
- Furthermore, the reliability rates quickly deteriorated as photographs went out of date, climbing to 15 per cent after only about 2 years for the best systems tested.[13] For governments that use the data to perform more ambitious one-to-many searches, tests show that the error rates would be sharply higher still.

- Implementation of facial recognition on a global scale is likely to increase these errors, and will lead to delays, duress, and confusion.
- Facial recognition technologies may reveal racial or ethnic origin.[14]
- The U.S. General Accounting Office warns that facial recognition is the only biometric that can be used for other surveillance applications, such as pinpointing individuals filmed on video cameras.[15]

We are very concerned that the New Orleans resolution permits individual countries to use multiple biometrics, such as iris scans and fingerprints *in addition to* facial recognition. These additional physical measures increase the likelihood that biometric databases will be used for other purposes. The New Orleans resolution is contrary to your stated goal of interoperability and allows countries to pursue invasive solutions using the ICAO standards as their excuse. We have already seen the EU propose a central fingerprint registry; others may follow.

The current plans to store the biometrics on 'contact-less integrated circuits' also raises a number of concerns. This is likely to involve the use of radio-frequency identification (RFID) chips. RFID-tagged passports could be secretly read right through a wallet, pocket, backpack, or purse by anyone with the appropriate reader device, including marketers, identity thieves, pickpockets, oppressive governments, and others. The ICAO is promoting the adoption of this technology even as RFID chips are stirring deep concerns and controversy around the world. It would be premature to finalize a choice of technology without consideration of these issues. Use of these chips must be re-considered, assessed, and compared with alternative technologies that are less invasive.

National biometric databases and the retention of biometrics by third-parties can be avoided. The ICAO could have been wiser in its selection of technology, and more specific in its implementation. Biometrics can be implemented in such ways that they are prevented from being used for surreptitious surveillance or tracking. Biometrics can be stored locally on travel documents, and border checks can simply verify the link between the individual's live biometric and the biometric template stored on the actual document. Such two-way checks have been considered by the ICAO,[16] but unfortunately are not part of the ICAO requirements. In addition, as EU privacy officials have written,

> biometric systems related to physical characteristics which do not leave traces (e.g. shape of the hand but not fingerprints) or biometrics systems related to physical characteristics which leave traces but do not rely on the memorisation of the data in the possession of someone other than the individual concerned (in other words, the data is not memorised in the control access device or in a central data base) create less risks for the protection for fundamental rights and freedoms of individuals.[17]

Such care in the creation of the standards has not been demonstrated by ICAO so far. The ICAO must go back and reconsider its choices and conduct a review of all available technologies and their likely effects on privacy and civil liberties.

Biometrics remains problematic even if implemented on a voluntary basis. Initiatives such as 'trusted traveller' and 'Simplified passenger travel' still create a surveillance infrastructure involving background checks and the transfer of personal information that can be used for additional purposes, including the protection of revenue control.[18] Those who fail to "volunteer" to subject themselves to increased surveillance will inevitably become second-class travellers subjected to more intrusive searching, longer lines and inconvenient delays.

What ICAO should do

The ICAO must impose restraints on the undue collection, processing, retention, and transfers of data. At the very least, we call on the ICAO to adopt specific requirements to ensure that countries do not use this mandate to build national biometric databases.

The current ICAO specifications are too broad, and would promote irresponsible national behaviour and allowing national governments to circumvent their own democratic deliberations on such sensitive issues as profiling, national identification cards, and international data-sharing.

Unless the ICAO is willing to propose only solutions that preserve privacy and human rights through its specification requirements for technological design and review alternative technologies, then we call on the ICAO to abandon its intent to adopt biometrics as a standard.

Specifically, the undersigned call on the ICAO to

- Follow through on earlier promises to review privacy implications of biometrics and trans-border personal information transfers;
- Release clear and binding privacy requirements that will reduce the risks of illegal collection, use, retention, and transfers of this information;
- Uphold national data protection laws or cultural practices, as previously promised by the ICAO;
- Prevent, by design or biometric selection, the development of biometric databases;
- Refrain from adopting RFID or biometric standards until their privacy and surveillance implications -- and the possibility that alternatives with less potential for privacy invasion or other abuse by surveillance agencies -- can be more fully evaluated.

We hope that the choices of biometrics have been driven primarily by logistical and commercial concerns, and were not intended to facilitate the conversion of travel systems into a global infrastructure of surveillance. But we are deeply concerned that this may become their unintended consequence.

Signed,

Privacy International

The American Civil Liberties Union

Statewatch

Association for Progressive Communications

European Digital Rights

International Civil Liberties Monitoring Group

Big Brother Awards Denmark (Denmark)

Big Brother Awards Switzerland (Switzerland)

Bits of Freedom (Netherlands)

British Columbia Civil Liberties Association (Canada)

British Columbia Freedom of Information and Privacy Association (Canada)

Center for Democracy and Technology (USA)

Community Communications Online (Australia)

Computer Professionals for Social Responsibility (USA)

Consumer Action (USA)

Consumers Against Supermarket Privacy Invasion and Numbering (USA)

Digital Rights (Denmark)

Electronic Frontier Canada (Canada)

Electronic Frontier Foundation (USA)

Electronic Privacy Information Center (USA)

The Foundation for Information Policy Research (UK)

FoeBuD e.V. (Germany)

GreenNet (UK)

IRIS - Imaginons un réseau Internet solidaire (France)

Korean Progressive Network Jinbonet (Korea)

La ligue des droits et libertés du Québec (Canada)

PrivacyActivism (USA)

Privacy Rights Clearinghouse (USA)

quintessenz (Austria)

STOP1984 (Germany)

Stand.org.uk (UK)

Swiss Internet User Group (Switzerland)

VIBE!AT (Austria)

ZaMirNET (Croatia)

---

[1] European Civil Aviation Conference, "Biometrics," (Cairo, Egypt: Presented to the ICAO summit in Cairo, 2004). See http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12ip002_en.pdf

[2] Colin Powell, "Subject: Enhanced Border Security and Visa Entry Reform Act of 2002 - Aldac No. 1," ed. ALL DIPLOMATIC AND CONSULAR POSTS, et al. (Washington, D.C.: Department of State, 2002). See http://travel.state.gov/state093239.html

[3] Thomas J. Ridge and Colin L. Powell, "Dear Mr. Chairman, Letter to the Chairman of the House Committee of the Judiciary," (Washington, D.C.: U.S. Congress, 2004). See http://www.house.gov/judiciary/ridge031704.pdf

[4] Commission of the European Communities, "Proposal for a Council Regulation on Standards for Security Features and Biometrics in EE Citizens' Passports," (Brussels: The European Commission, 2004). See http://register.consilium.eu.int/pdf/en/04/st06/st06406-re01.en04.pdf

[5] French Government, "Implementation of Biometric Techniques on French Airports," (Cairo, Egypt: Presented to the ICAO summit in Cairo, 2004). See http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12ip024_en.pdf

[6] ICAO, "Biometrics Deployment of Machine Readable Travel Documents ICAO TAG MRTD/NTWG Technical Report: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation Using Machine Readable Travel Documents," (Montreal: ICAO, 2003).

[7] Council of European Union, "Commission Paper on Terrorism to the Council: Providing Input for the European Council," (Brussels: Note from Secretary-General of the European Commission, signed by Mrs Patricia BUGNOT, Director, to Mr Javier SOLANA, Secretary-General/High Representative, Subject: Commission paper to the Council on Terrorism providing input for the European Council, 2004).

[8] Commission of the European Communities, "Proposal for a Council Regulation on Standards for Security Features and Biometrics in EU Citizens' Passports."

[9] Ibid. With the larger chip-size, the EU can go even further than two biometrics. As the proposed regulation says, "However, as it may be necessary to store a facial image and fingerprint images, a 64 K chip would be more appropriate, especially if Member States wish to add some alphanumeric data."

[10] Article 29 Working Party, "Working Document on Biometrics," (Brussels: European Commission, 2003). See http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf

[11] European Civil Aviation Conference, "Biometrics."

[12] GAO, "Challenges in Using Biometrics: A Testimony for the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives," (Washington, D.C.: General Accounting Office, 2003).

[13] United States Government, "Face Recognition for Identity Confirmation -- Inspection of Travel Documents," (Cairo, Egypt: Presented to the ICAO summit in Cairo, 2004). See http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp063_en.pdf

[14] Article 29 Working Party, "Working Document on Biometrics."

[15] GAO, "Challenges in Using Biometrics: A Testimony for the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives."

[16] ICAO, "Biometrics Deployment of Machine Readable Travel Documents ICAO TAG MRTD/NTWG Technical Report: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation Using Machine Readable Travel Documents."

[17] Ibid.

[18] According to IATA "The use of biometrics as an identity authentication and entitlement function will result in more confidence in revenue control, and the ability to know with more certainty, exactly who is getting onto flights.". For more information see "Accelerating a Worldwide Approach to Biometric Identity Confirmation in MRTDs as the Key Token of Entitlement for Simplified Passenger Travel," (Cairo, Egypt: International Air Transport Association (IATA) presentation to the ICAO Cairo summit, 2004). See http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12ip007_en.pdf