



Privacy International

The Rt Honourable Kunio Hatoyama  
Minister of Justice  
1-1-1 Kasumigaseki  
Chiyoda-ku, Tokyo  
Nippon

November 19, 2007

Dear Minister Hatoyama

Regarding plans to fingerprint and face-scan all visitors to Japan

We, the undersigned human rights and civil liberties groups from around the world are writing to you to express our grave concerns regarding the Ministry of Justice's imminent implementation of the Immigration Control and Refugee Recognition Act.

We believe that your plans to fingerprint and face-scan foreign-residents and visitors to Japan are a gross and disproportionate infringement upon civil liberties, copying the most ineffective, costly and risky practices on border management from around the world.

We respectfully call on you to reconsider your plans to implement this system. We also call on you to explain to the world why potential visitors should travel to your country and face these inconveniences when you have done so little to explain the nature of this human processing. We believe it is likely that the implementation of this system will create a negative impact on your tourism industry and on the flow of foreign workers to Japan, thus hurting Japan's economy and in turn giving rise to possible claims of Japanese isolationism.

### **Background**

According to your plans for Immigration Control:

"In order to detect and oust, at the border, terrorists or foreign nationals who have been deported from Japan or committed crimes, one effective method is to further enhance measures against forged and falsified documents and to utilize biometrics in immigration examinations.

In order to take facial portraits and fingerprint data during landing examinations of foreign nationals under the "Action Plan for Prevention of Terrorism" (as adopted at the Headquarters for Promotion of Measures Against Transnational Organized Crime

6-8 Amwell Street  
London  
EC1R 1UQ, GB  
[gus@privacy.org](mailto:gus@privacy.org)  
<http://www.privacyinternational.org>

and Other Relative Issues and International Terrorism on December 10, 2004), necessary preparations will be made by putting in order points for us to keep in mind, observing relevant measures taken by foreign countries and developing relevant law."<sup>1</sup>

It has come to our attention that you plan to implement this system within a matter of weeks that you will face-scan and fingerprint all visitors to Japan and retain this information for an extended period of time (some reports claim that you intend to do so for up to 80 years), and combine this data with other sources of personal information.

### **Infringing upon the Right to Privacy**

Your plans are in breach of individuals' human rights, and in particular, their right to privacy. The right to privacy is recognized specifically by numerous international human rights treaties. The Universal Declaration of Human Rights recognises the right to privacy under Article 12. Similar language is adopted in the International Covenant on Civil and Political Rights under Article 17, the United Nations (UN) Convention on Migrant Workers in Article 14, and the UN Convention on the Rights of the Child under Article 16. We note that the Japanese Supreme Court has recognized the right to privacy under Article 13 of the Japanese Constitution.

Your system proposes to indiscriminately collect sensitive personal information from all foreign travellers. This mass project for the processing of human beings is tantamount to treating all visitors to your country as though they were criminals.

We are surprised by the lack of information regarding proposed safeguards and appeal methods. Instead we hear rhetoric about the importance of combating terrorism and threats to force the return of anyone who fails to comply with this new requirement.

This is particularly worrisome because Japan's privacy laws are regarded as weak by international standards. We note that Japan has to some extent applied international standards such as the OECD's Privacy Guidelines into two recent privacy laws. The law that covers commercial entities partially follows international standards, yet the law that applies to the use and sharing of data held by government

---

<sup>1</sup> Ministry of Justice, 'Basic Plan for Immigration Control (3rd Edition) provisional translation', Section 3: Major Issues and Guidelines on Immigration Control Administration Services, available at <<http://www.moj.go.jp/ENGLISH/information/bpic3rd-03.html#3-2-1-B>>

agencies is very weak. This decreases our confidence that your government has the necessary accountability structures to collect such vast amounts of personal information.

The protection of human rights is at its weakest when individuals are waiting for entry at the border of a foreign country. Traditionally, governments afforded respect to visitors from other nations on the basis of reciprocity: if you treat one nation's citizens with respect that nation's government will treat yours similarly. Japan is showing a remarkable level of disrespect to the dignity of tourists and foreign business travellers by collecting detailed information on them, in an indiscriminate manner as a condition of entry, with no promise of safeguards, or any means of appeal.

We also note that the Japanese Government previously criticised systems such as the one you are about to implement. In 2002 at a meeting of the International Civil Aviation Organisation the Japanese delegation stated that "the Japanese people are saddened by the approach of the United States", and the delegation could not understand "why the United States can not longer trust Japanese citizens" and that the unilateral use of biometrics will have a negative impact on the 17 million Japanese that visit the U.S. every year.<sup>2</sup> We are surprised by this turn of events and opinion.

### **A Complex and Risky System**

The collection of all this personal information and its centralisation into databases will create privacy risks, and will also lead to likely security risks.

We believe that Japan is making a grave mistake by following the path forged by the United States of America with its US-VISIT programme. Until the implementation of your system, the U.S. was alone in the world in fingerprinting and face-scanning all visitors and retaining this information for vast periods of time. Years into their programme it is clear that the U.S. should serve as a cautionary tale rather than as an example of best practice.

The US-VISIT system was approved in a similar manner to the Japanese system. That is, it was approved through a highly political environment with little public debate or policy deliberation. In the U.S.,

---

<sup>2</sup> 'Notes from Meeting of ICAO New Technologies Working Group', Berlin, Germany, June 25-28, 2002, documents unclassified by the U.S. Department of State in August 2004.

the government relied on its rhetoric about fighting terrorism and crime rather than careful policy development and deployment. Now, years later, the US-VISIT system is finally receiving some of its much needed oversight, and the reality of advanced border systems is becoming clear. According to U.S. Government reports, we now know that:

- after spending \$1.3 billion over 4 years, only half the U.S. system has been delivered.<sup>3</sup>
- expenditures continue on projects that "are not well-defined, planned, or justified on the basis of costs, benefits, and risks", lacking "a sufficient basis for effective program oversight and accountability".<sup>4</sup>
- the U.S. government has "continued to invest in US-VISIT without a clearly defined operational context that includes explicit relationships with related border security and immigration enforcement initiatives".<sup>5</sup>
- "management controls to identify and evaluate computer and operational problems were insufficient and inconsistently administered" and thus "continues to face longstanding US-VISIT management challenges and future uncertainties" as it continues to "fall short of expectations".<sup>6</sup>
- "lacking acquisition and financial management controls", and project managers have failed to "economically justify its investment in US-VISIT increments or assess their operational impacts", "had not assessed the impact of the entry and exit capabilities on operations

---

<sup>3</sup> Government Accountability Office, Prospects For Biometric US-VISIT Exit Capability Remain Unclear, July 28, 2007, GAO-07-1044T.

<sup>4</sup> Government Accountability Office, 'U.S. Visitor and Immigrant Status Program's Long-standing Lack of Strategic Direction and Management Controls Needs to Be Addressed', August 2007, GAO-07-1065.

<sup>5</sup> Government Accountability Office, 'Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified', February 2007, GAO-07-278.

<sup>6</sup> Government Accountability Office, 'US-VISIT Program Faces Operational, Technological, and Management Challenges', March 20, 2007, GAO-07-623T.

and facilities, in part, because the scope of the evaluations performed were too limited."<sup>7</sup>

- "contracts have not been effectively managed and overseen".<sup>8</sup>
- and finally, security "weaknesses collectively increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information, including personally identifiable information, and disrupt the operations of the US-VISIT program." According to the chairman of the U.S. Senate Homeland Security Committee, Senator Joseph Lieberman, the U.S. government "is spending \$1.7 billion of taxpayer money on a program to detect potential terrorists crossing our borders yet it isn't taking the most basic precautions to keep them from hacking into and changing or deleting sensitive information."<sup>9</sup>

It is therefore of little surprise that the U.S. border systems occasionally fail. On a number of occasions the U.S. border systems have broken down resulting in thousands of people being forced to wait until the system problems could be resolved. For instance, in August 2007, 20,000 travellers were left stranded at Los Angeles airport, with visitors spending the night on the airport floors and planes prevented from even coming into the gates for passengers (both citizens and visitors) to de-plane because the airport was overwhelmed.<sup>10</sup>

More stories are emerging from around the world where weak security protocols have made personal information held on visa databases widely available to the public and potential identity thieves,<sup>11</sup> and where fingerprint mismatches have led to gross injustices. Without competent planning and care, visitors to Japan have no reason to be

---

<sup>7</sup> Government Accountability Office, US-VISIT Has Not Fully Met Expectations and Longstanding Program Management Challenges Need to Be Addressed, February 16, 2007, GAO-07-499T.

<sup>8</sup> Government Accountability Office, 'Contract Management and Oversight for Visitor and Immigrant Status Program Need to Be Strengthened', June 2006, GAO-06-404.

<sup>9</sup> 'Lieberman Cites Vulnerability of Terrorism Tracking Data', August 3, 2007, statement available at <<http://lieberman.senate.gov/newsroom/release.cfm?id=280527&&>>.

<sup>10</sup> 'Mayor calls for Probe of LAX Computer Crash', CBS, August 13, 2007.

<sup>11</sup> 'Security concerns hit web visa applications', Joe Churcher, The Scotsman, May 18, 2007.

confident that the personal information that they are forced to disclose will be adequately protected by your system.

### **Towards Effective Border Management?**

Japan should be careful not to follow the U.S. lead. Recent surveys have shown that the U.S. is now rated as the worst place to visit because of its immigration and entry procedures, followed by the Middle East.<sup>12</sup>

There are better ways of greeting visitors to your country than treating tourists and business travelers as though they were terrorists. There are privacy-friendly ways of identifying criminals at borders without invading the privacy of all visitors and making them vulnerable to identity theft through the leakage of data from your systems.

For instance, border officials could verify passports against the INTERPOL list of lost and stolen passports from around the world. Remarkably so few countries actually do this. It would be a far more effective and proportionate solution.

Even this step must be made with great care as errors are still likely which will inhibit the flow of travellers. As an example, in a test of 1.9 million passport records collected over 16 days by U.S. border officials, 273 documents were identified as stolen documents. Eventually however, 219 cases were cleared and 64 remained unresolved. As with any watchlist program, clear oversight and accountability structures must be established to allow for the necessary appeals against erroneous data. We have already seen numerous problems with the U.S. watchlists wrongly flagging innocent individuals as terrorists, growing out of control with serious integrity problems.<sup>13</sup> We expect that any system your government implements will likely give rise to similar problems.

In our experiences, technological systems fail most when they do not receive adequate policy deliberation. We also believe that immigration policy is a complex domain that rarely attracts the necessary attention

---

<sup>12</sup> 'How to help the huddled masses through immigration', Gideon Rachman, Financial Times, March 12, 2007.

<sup>13</sup> Statement of Glenn A. Fine, Inspector General, U.S. Department of Justice, before the House Committee on Homeland Security concerning The Terrorist Screening System and the Watchlist Process, November 8, 2007, available at <http://www.usdoj.gov/oig/testimony/t0711/final.pdf>.

and deliberative care that it deserves. Your plans to fingerprint and face-scan every visitor to your country appears to exemplify this risk. It is unfortunate that we could not offer our views earlier but your consultation was only conducted in the Japanese language.

Your plans will damage Japan's standing in the world, making a wonderful and beautiful country less inviting to tourists, and will unnecessarily hurt Japan's role as a global economic leader. If serious changes to your plans are not made, we worry that individuals who are concerned about the privacy and security of their personal information will avoid travel to Japan.

Please reconsider your plans. Also, please note, that if you move down this path, other governments may well follow and will start fingerprinting your own citizens on the grounds that you do it to theirs. These systems will likely be as complex, risky and insecure as yours. This is not the type of world that you, your citizens or we would like to live in.

Yours sincerely,

Privacy International

Action on Rights for Children (UK)  
APC Africa Women (Africa)  
APC.au (Australia)  
ArabDev (Egypt)  
Asian Coalition for Housing Rights (Japan)  
Association For Progressive Communications (International)  
Associazione per la Libertà nella Comunicazione Elettronica Interattiva (Italy)  
ATTAC Japan (Japan)  
Australian Privacy Foundation (Australia)  
AZUR Developpement (Congo)  
Big Brother Awards (France)  
Bluelink (Bulgaria)  
British Columbia Civil Liberties Association (Canada)  
BytesForAll.org (South Asia)  
Canadian Internet Policy and Public Interest Clinic (Canada)  
Colnodo (Colombia)  
Community Education Computer Society (South Africa)  
Digital Rights (Denmark)  
Digital Rights Ireland  
Electronic Frontier Finland (Finland)

Electronic Frontier Foundation (US)  
Electronic Privacy Information Center (US)  
European Digital Rights (EU)  
Fantsuam Foundation (Nigeria)  
Focus on the Global South (Asia)  
Foundation for Information Policy Research (FIPR)  
Foundation For Media Alternatives (Philippines)  
GreenNet (UK)  
Greenspider (Hungary)  
Index on Censorship (International)  
International Civil Liberties Monitoring Group (International)  
International Movement Against All Forms of Discrimination and Racism (Japan)  
International Solidarity Action of the Have-Nots (Japan)  
IRIS - Imaginons un réseau Internet solidaire (France)  
Iuridicum Remedium (Czech Republic)  
Japan Computer Access for Empowerment (Japan)  
Japan Lawyers Network for Refugees (Japan)  
JCA-NET(Japan)  
Jinbonet (South Korea)  
Joint Labor Union of Christian Offices and Businesses (Japan)  
Laneta (Mexico)  
Network Against JUKINET(Japan)  
Networkers against Surveillance Task-force (Japan)  
Netzwerk Neue Medien (Germany)  
No2ID (UK)  
NODO Tau (Argentina)  
OneWorld Platform South West Europe (Bosnia-Herzegovina)  
Open Rights Group (UK)  
Peace Boat (Japan)  
Peace Not War Japan (Japan)  
People's Coalition against Wiretapping Law and Organized Crime Law (Japan)  
People's Plan Study Group(PPSG) (Japan)  
PINCH! Against War and Surveillance (Japan)  
Privacy Journal (US)  
RITS - Information Network for the Third Sector (Brazil)  
San'ya Welfare Center for Day-Laborers' Association (Japan)  
Sex Worker and Sexual Health (Japan)  
Solidarity Network with Migrants Japan (Japan)  
Statewatch (UK)  
StrawberryNet (Romania)  
Swiss Association to Defend Fundamental Rights (Switzerland)  
Swiss Internet User Group (Switzerland)  
Ungana Afrika (Africa)  
VOICE (Bangladesh)  
Wamani (Argentina)  
WiLAC (Uruguay)  
WomensNet (South Africa)

