Case Id: ac9aea63-a6a9-40f3-841b-599cd6672778
Date: 29/10/2015 23:51:26

Public Consultation on the Smart Borders Package

Fields marked with * are mandatory.

Questions to all contributors

* You are responding this questionnaire as:
  - (●) An individual
  - ( ) A public authority
  - ( ) An organisation (non-governmental, civil society organisation, academia, research, social partner, interest group, consultancy, think-tank...)
  - ( ) A carrier, transport or tourism operator, or a transport infrastructure operator

* Contributions received from this survey will be published on the European Commission's website (for further information, please consult the privacy statement). Do you agree your contribution being published?
  - ( ) Yes, your contribution may be published under your name (or the name of the entity you represent)
  - (●) Yes, your contribution may be published but should be kept anonymous (without your name or the name of the entity you represent)
  - ( ) No, you do not want your contribution to be published. Your contribution will not be published, but it may be used internally within the Commission for statistical and analytical purposes

Questions to individuals

1. General information — your profile

* First name: (maximum 100 characters)

Text of 1 to 100 characters will be accepted

* Surname: (maximum 100 characters)

Text of 1 to 100 characters will be accepted

* Email address: (maximum 100 characters)

Text of 1 to 100 characters will be accepted

* Occupation: (maximum 100 characters)

Text of 1 to 100 characters will be accepted

artist

* Nationality:

between 1 and 3 choices

- [ ] Afghanistan
- [ ] Albania
- [ ] Algeria
- [ ] Andorra
- [ ] Angola
- [ ] Antigua and Barbuda
- [ ] Argentina
- [ ] Armenia
- [ ] Australia
- [ ] Austria
- [ ] Azerbaijan
- [ ] Bahamas
- [ ] Bahrain
- [ ] Bangladesh
- [ ] Barbados
- [ ] Belarus
- [ ] Belgium
- [ ] Belize
- [ ] Benin
- [ ] Bhutan
- [ ] Bolivia
- [ ] Bosnia and Herzegovina
- [ ] Botswana
- [ ] Brazil
- [ ] Brunei
- [ ] Bulgaria
- [ ] Burkina Faso

- [ ] Burma
- [ ] Burundi
- [ ] Cambodia
- [ ] Cameroon
- [ ] Canada
- [ ] Cape Verde
- [ ] Central African Republic
- [ ] Chad
- [ ] Chile
- [ ] China
- [ ] Colombia
- [ ] Comoros
- [ ] Congo
- [ ] Costa Rica
- [ ] Côte d'Ivoire
- [ ] Croatia
- [ ] Cuba
- [ ] Cyprus
- [ ] Czech Republic
- [ ] Democratic Republic of the Congo
- [ ] Denmark
- [ ] Djibouti
- [ ] Dominica
- [ ] Dominican Republic
- [ ] East Timor
- [ ] Ecuador
- [ ] Egypt
- [ ] El Salvador
- [ ] Equatorial Guinea
- [ ] Eritrea
- [ ] Estonia
- [ ] Ethiopia
- [ ] Fiji
- [ ] Finland
- [ ] former Yugoslav Republic of Macedonia
- [ ] France
- [ ] Gambia
- [ ] Georgia
- [ ] Germany
- [ ] Ghana
- [ ] Greece
- [ ] Grenada
- [ ] Guatemala
- [ ] Guinea
- [ ] Guinea-Bissau
- [ ] Guyana

- [ ] Haiti
- [ ] the Holy See/Vatican City State
- [ ] Honduras
- [ ] Hong Kong
- [ ] Hungary
- [ ] Iceland
- [ ] India
- [ ] Indonesia
- [ ] Iran
- [ ] Iraq
- [ ] Ireland
- [ ] Israel
- [ ] Italy
- [ ] Jamaica
- [ ] Japan
- [ ] Jordan
- [ ] Kazakhstan
- [ ] Kenya
- [ ] Kiribati
- [ ] Kosovo
- [ ] Kuwait
- [ ] Kyrgyzstan
- [ ] Laos
- [ ] Latvia
- [ ] Lebanon
- [ ] Lesotho
- [ ] Liberia
- [ ] Libya
- [ ] Liechtenstein
- [ ] Lithuania
- [ ] Luxembourg
- [ ] Macao
- [ ] Madagascar
- [ ] Malawi
- [ ] Malaysia
- [ ] Maldives
- [ ] Mali
- [ ] Malta
- [ ] Marshall Islands
- [ ] Mauritania
- [ ] Mauritius
- [ ] Mexico
- [ ] Micronesia
- [ ] Moldova
- [ ] Monaco
- [ ] Mongolia

- [ ] Montenegro
- [ ] Montserrat
- [ ] Morocco
- [ ] Mozambique
- [ ] Namibia
- [ ] Nauru
- [ ] Nepal
- [ ] Netherlands
- [ ] New Zealand
- [ ] Nicaragua
- [ ] Niger
- [ ] Nigeria
- [ ] North Korea
- [ ] Norway
- [ ] Oman
- [ ] Pakistan
- [ ] Palau
- [ ] Palestinian Authority
- [ ] Panama
- [ ] Papua New Guinea
- [ ] Paraguay
- [ ] Peru
- [ ] Philippines
- [ ] Poland
- [ ] Portugal
- [ ] Qatar
- [ ] Romania
- [ ] Russia
- [ ] Rwanda
- [ ] Saint Kitts and Nevis
- [ ] Saint Lucia
- [ ] Saint Vincent and the Grenadines
- [ ] Samoa
- [ ] San Marino
- [ ] São Tomé and Príncipe
- [ ] Saudi Arabia
- [ ] Senegal
- [ ] Serbia
- [ ] Seychelles
- [ ] Sierra Leone
- [ ] Singapore
- [ ] Slovakia
- [ ] Slovenia
- [ ] Solomon Islands
- [ ] Somalia
- [ ] South Africa

- [ ] South Korea
- [ ] South Sudan
- [ ] Spain
- [ ] Sri Lanka
- [ ] Sudan
- [ ] Suriname
- [ ] Swaziland
- [ ] Sweden
- [ ] Switzerland
- [ ] Syria
- [ ] Taiwan
- [ ] Tajikistan
- [ ] Tanzania
- [ ] Thailand
- [ ] Togo
- [ ] Tonga
- [ ] Trinidad and Tobago
- [ ] Tunisia
- [ ] Turkey
- [ ] Turkmenistan
- [ ] Tuvalu
- [ ] Uganda
- [ ] Ukraine
- [ ] United Arab Emirates
- [ ] United Kingdom
- [x] United States
- [ ] Uruguay
- [ ] Uzbekistan
- [ ] Vanuatu
- [ ] Venezuela
- [ ] Vietnam
- [ ] Yemen
- [ ] Zambia
- [ ] Zimbabwe
- [ ] Other

* Country of residence:

- ( ) Afghanistan
- ( ) Albania
- ( ) Algeria
- ( ) Andorra
- ( ) Angola
- ( ) Antigua and Barbuda
- ( ) Argentina

- Armenia
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bhutan
- Bolivia
- Bosnia and Herzegovina
- Botswana
- Brazil
- Brunei
- Bulgaria
- Burkina Faso
- Burma
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Central African Republic
- Chad
- Chile
- China
- Colombia
- Comoros
- Congo
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Cyprus
- Czech Republic
- Democratic Republic of the Congo
- Denmark
- Djibouti
- Dominica
- Dominican Republic
- East Timor
- Ecuador

- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Ethiopia
- Fiji
- Finland
- former Yugoslav Republic of Macedonia
- France
- Gambia
- Georgia
- Germany
- Ghana
- Greece
- Grenada
- Guatemala
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- the Holy See/Vatican City State
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Israel
- Italy
- Jamaica
- Japan
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho

- Liberia
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macao
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Mauritania
- Mauritius
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Namibia
- Nauru
- Nepal
- Netherlands
- New Zealand
- Nicaragua
- Niger
- Nigeria
- North Korea
- Norway
- Oman
- Pakistan
- Palau
- Palestinian Authority
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Qatar

- ○ Romania
- ○ Russia
- ○ Rwanda
- ○ Saint Kitts and Nevis
- ○ Saint Lucia
- ○ Saint Vincent and the Grenadines
- ○ Samoa
- ○ San Marino
- ○ São Tomé and Príncipe
- ○ Saudi Arabia
- ○ Senegal
- ○ Serbia
- ○ Seychelles
- ○ Sierra Leone
- ○ Singapore
- ○ Slovakia
- ○ Slovenia
- ○ Solomon Islands
- ○ Somalia
- ○ South Africa
- ○ South Korea
- ○ South Sudan
- ○ Spain
- ○ Sri Lanka
- ○ Sudan
- ○ Suriname
- ○ Swaziland
- ○ Sweden
- ○ Switzerland
- ○ Syria
- ○ Taiwan
- ○ Tajikistan
- ○ Tanzania
- ○ Thailand
- ○ Togo
- ○ Tonga
- ○ Trinidad and Tobago
- ○ Tunisia
- ○ Turkey
- ○ Turkmenistan
- ○ Tuvalu
- ○ Uganda
- ○ Ukraine
- ○ United Arab Emirates
- ○ United Kingdom
- ◉ United States

- Uruguay
- Uzbekistan
- Vanuatu
- Venezuela
- Vietnam
- Yemen
- Zambia
- Zimbabwe
- Other

* Are you:
- An EU citizen
- A non-EU citizen visiting or intending to visit the Schengen area for a short stay (less than 90 days within a period of 180 days)
- A non-EU citizen resident in the EU
- Other

* Your are visiting or intending to visit the Schengen area for a short stay for:
- Tourism
- Business/professional reasons
- A political, scientific, cultural, sports or religious event
- Family visit
- Other

* If you are a non-EU citizen visiting the Schengen area for a short stay, do you hold a visa? (question only for non-EU citizens visiting the Schengen area for a short stay)
- Yes, a single entry visa
- Yes, a multiple entry visa
- No

* If you are not an EU citizen, have you ever travelled to the Schengen area? (question only for non-EU citizens visiting the Schengen area for a short stay)
- Yes
- No

* If you are not an EU citizen, how often do you travel to the Schengen area? (question only for non-EU citizens)
- Less than once a year
- 1-2 times a year
- 3-5 times a year
- 6-10 times a year
- More than 10 times a year

2. The use of biometric identifiers

* The 2013 legislative proposal on the Entry/Exit System requires visa-exempt non-EU citizens e ntering the Schengen area for a short stay to give 10 fingerprints at the border crossing if they are not registered in the Entry/Exit System — either because it is their first visit or because the data retention period has expired since their last visit.
Travellers who hold a visa will have given fingerprints when applying for it, so would not need to have their fingerprints taken again at border crossings.
The 2013 legislative proposal on the Registered Traveller Programme requires non-EU citizens applying for the programme to give four fingerprints. They would give these when submitting an application under the programme.
Both proposals exempt children under the age of 12 from the requirement to give their fingerprints.
In both cases, biometric identifiers (fingerprints) would be used to improve on identity and verification checks, e.g. to verify that the person crossing the border is the person to whom the passport was issued. The Commission is currently examining the feasibility of using other types of biometric identifiers (in particular photo/'facial image') for this purpose.

What kind of biometric identifiers would you prefer to be used?

- (●) No biometrics at all, only alphanumerical data (for example, your name, surname and travel document number)
- ( ) Fingerprints only
- ( ) A combination of facial image and a limited number of fingerprints
- ( ) Facial image only

* Why? Please explain: (maximum 500 characters)

Text of 1 to 500 characters will be accepted

see the document at
https://www.scribd.com/doc/287786277/EC-Public-Consultation-on-Smart-Borders-Oct-29-2015

* If you are not an EU citizen, would you be dissuaded from travelling to the Schengen area if you had to give fingerprints? (question only for non-EU citizens)

- (●) Yes
- ( ) No

* If you are not an EU citizen, would you be dissuaded from travelling to the Schengen area if your facial image was used? (question only for non-EU citizens)

- (●) Yes
- ( ) No

* Do you think that the use of biometric identifiers could jeopardise or improve the reliability of border checks?

- (●) Jeopardise
- ( ) Improve
- ( ) No opinion / Not sure

* Please explain: (maximum 500 characters)

Text of 1 to 500 characters will be accepted

see the document at
https://www.scribd.com/doc/287786277/EC-Public-Consultation-on-Smart-Borders-Oct-29-2015

3. Process to accelerate border crossing for non-EU citizens

* The 2013 proposal for the Registered Traveller Programme proposes setting up a programme to enable pre-vetted non-EU citizens to benefit from facilitations at borders. This will make it easier and quicker for these pre-vetted frequent travellers to cross borders. The Commission is analysing potential simplifications to this approach.

To what extent do you consider that there is a need for a process to accelerate border crossings by non-EU citizens at the Schengen area's external borders?

- ○ To a great extent
- ○ To some extent
- ◉ To a small extent
- ○ Not at all
- ○ I do not know

* The 2013 proposal for the Registered Traveller Programme provides for a faster border crossing process for those travellers having submitted a specific application. Applicants for the Registered Traveller Programme would be subject to some specific checks when submitting their application. Participation in the programme would require the payment of a fee. For their subsequent journeys, accepted Registered Travellers would be exempt from part of the checks applicable at borders to non-EU citizens. At major external border crossing points equipped with automated border control gates, border checks would be performed using these infrastructures. Where no automated border control gates would be available, Registered Travellers would be able to use the lanes reserved for citizens of EU countries and Iceland, Liechtenstein, Norway and Switzerland.

(A) Do you consider that this specific process to accelerate border crossings should be available for non-EU citizens?

- ○ Yes
- ◉ No

* Why? Please explain: (maximum 500 characters)

Text of 1 to 500 characters will be accepted

Having a system whereby individuals give up more information in order to go through borders faster incentivises immigration authorities to slow borders down in order to collect more information on travelers. This conflict of interest is too powerful to ignore.

There is a second conflict of interest: ABC gates and passports are often manufactured by the same company. They will make decisions which make sense for their needs, but often are bad for the security of the documents/people.

* (B) If you are not an EU citizen, would you be personally interested in this process? (Question only for non-EU citizens)

- ○ Yes
- ◉ No

* Why? (You may tick more than one box)

- ☐ I do not travel enough, so do not need it
- ☐ I do not want to submit an application
- ☑ Other

* Please explain: (maximum 500 characters)

Text of 1 to 500 characters will be accepted

I wouldn't give up my security (in the form of biometric data which could be lost by the EU) in order to make the border crossing process go faster.

* Another faster border crossing process could be envisaged for those travellers entering the Schengen area for a short stay and whose passport data and biometric identifiers had already been registered in:

- the Visa Information System for travellers holding a short-stay visa;

- the Entry/Exit System for visa-exempt travellers whose data has been registered during a previous journey, if the retention period has not yet expired.

These travellers would be able to benefit from a faster process without needing to submit any application. This process would be available at those border crossing points equipped with self-service kiosks. Some elements of the border checks (passport control, biometric verification, answering questions...) could be performed using self-service kiosks. The decision to authorise or refuse entry would be taken by a border guard who may also need to talk to the traveller for additional verifications.

(A) Do you consider that the process to accelerate border crossings described above should be available for the two categories of travellers listed?

- ○ Yes
- ◉ No

* Please explain: (maximum 500 characters)

Text of 1 to 500 characters will be accepted

> Having a system whereby individuals give up more information in order to go through borders faster incentivises immigration authorities to slow borders down in order to collect more information on travelers. This conflict of interest is too powerful to ignore.
>
> There is a second conflict of interest: self-service kiosks and passports are often manufactured by the same company. They will make decisions which make sense for their needs, but often are bad for the security of the documents/people

* (B) If you are not an EU citizen, would you be personally interested in this process? (Question only for non-EU citizens)

- ○ Yes
- ◉ No

* Why? (you may tick more than one box)

- ☑ I do not want to use a self-service kiosk
- ☑ I do not need to reduce the time taken by border checks
- ☐ I do not travel enough so do not need this
- ☑ Other

* Please explain: (maximum 500 characters)

Text of 1 to 500 characters will be accepted

I wouldn't give up my security (in the form of biometric data which could be lost by the EU) in order to make the border crossing process go faster.

* If you needed to apply for the faster border crossing procedure under the Registered Traveller Programme, would you prefer to submit your application and supporting documents: (question only for non-EU citizens)

- ○ Online
- ○ In person (for instance at a Member State's consulate or at an external border crossing point)
- ○ Both options should be possible
- ◉ No preference

* The 2013 proposal for the Registered Traveller Programme requires applicants to pay a fee. If accepted, registration would be granted for one year. Registration could be extended twice for two years (to five years in total) without further payment. Would you be ready to pay this fee? (only for non-EU citizens)

- ○ Yes
- ○ No
- ◉ No opinion / Not sure

* The use of self-service kiosks would require you to scan your travel document and to answer some questions on a screen or using a keyboard. Depending on the biometric identifier chosen (fingerprints, facial image or a combination of fingerprints and facial image), the use of self-service kiosks would also require you to place one or more of your fingers on a biometric reader and/or to have a picture of your face taken automatically. If self-service kiosks were available at border crossing points, would you be interested in using them to accelerate border crossing? (question only for non-EU citizens)

- ○ Yes
- ◉ No
- ○ No opinion / Not sure

* Please explain: (You may tick more than one box)

- ☐ I find it complicated to use self-service kiosks
- ☐ I am afraid of making a mistake
- ☐ I don't want to put my fingers on a self-service kiosk (for hygienic reasons)
- ☑ I don't want to use a self-service kiosk to have a picture of my face taken
- ☐ The use of self-service kiosks might result in inconvenient delay
- ☑ Other

* Please explain: (maximum 500 characters)

Text of 1 to 500 characters will be accepted

I wouldn't give up my security (in the form of biometric data which could be lost by the EU) in order to make the border crossing process go faster.

4. Data

* The 2013 Entry/Exit System proposal sets a limit to how long data can be kept after its collection at the entry and exit of the Schengen area's external borders:
1) A maximum retention period of 181 days after exit (91 days if the traveller has been absent from the Schengen area for 90 days). This retention period enables enforcement of the rule authorising non-EU citizens to stay in the Schengen area during 90 days within any period of 180 days.
2) A data retention period of five years for a person who has overstayed (i.e. remains in the Schengen area beyond the authorised period of stay). This data retention period aims to support the identification of the person and the return to his/her country of origin.
The Commission is evaluating whether these retention periods should be adapted in its new proposal.

Concerning the data retention period for the Entry/Exit System for non-overstayers, would you be in favour of:

- (●) A maximum data retention period of 181 days starting from the exit date. This period is sufficient to calculate the duration of authorised short stays in the Schengen
- ( ) A longer data retention period, to speed up border controls as a traveller returning to the Schengen area during the data retention period would not need to re-enrol under the Entry/Exit System, since his/her personal data is still stored in the system and can be reused.
- ( ) Other

* Concerning the data retention period for the Entry/Exit System for people who overstay, would you be in favour of:

- ( ) A data retention of five years following the last day of the authorised stay
- ( ) A data retention longer than five years
- (●) A data retention shorter than five years

* Why? Please explain: (maximum 500 characters)

Text of 1 to 500 characters will be accepted

If the goal of the project is to identify overstays, once a person is known to have left Schengen, what is the basis for maintaining the data?

5. Law enforcement access to the Entry/Exit System data

* The 2013 Entry/Exit System proposal provides that the option for law enforcement authorities to access data will be evaluated two years after the system enters into operation.
For its forthcoming revised proposal, the Commission is analysing whether law enforcement authorities should have access to the system, and if so, under which conditions. This analysis will address the necessity, appropriateness and proportionality of this option and be accompanied by a fundamental rights impact assessment.

Would you favour granting law enforcement authorities access to the data stored in the Entry/Exit System for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences? This access would be granted under strict legal prerequisites in full compliance with fundamental rights.

- ○ Yes
- ◉ No
- ○ Not yet. The issue should be evaluated two years after the implementation of the Entry/Exit System
- ○ No opinion / Not sure

* Please explain why: (You may tick more than one box)

- ☑ There is no need for such access
- ☐ Other

* If law enforcement authorities had access to the Entry/Exit System data, which of the following conditions should be implemented to mitigate the impact on fundamental rights and in particular on data protection? (You may tick more than one box)

- ☑ Access should be limited to the prevention, detection or investigation of terrorist offences or other serious criminal offences.
- ☑ There should be reasonable grounds to consider that the specific envisaged consultation of the Entry/Exit System data will substantially contribute to the prevention, detection or investigation of any of the terrorist or serious criminal offences in question.
- ☑ Searches should only be possible in specific cases under clearly defined circumstances. The proposal should exclude searches on a systematic basis.
- ☑ The data should be accessible for law enforcement purposes for a predefined limited period of time.
- ☑ A court or an independent administrative body should verify in each case if the required conditions for consulting the Entry/Exit System for law enforcement purposes are fulfilled.
- ☑ Access to the Entry/Exit System should only be possible if prior searches in more restricted databases (e.g. Member States' criminal databases) do not provide sufficient results.
- ☑ No opinion / Not sure.
- ☐ Other

6. Stamping — Questions only for non-EU citizens

* Currently, stamping the passport is the only method of indicating the dates and locations of entry and exit. The stamps are used by border guards and immigration authorities to calculate the duration of the stay of non-EU citizens and to verify compliance with the rules on short stay (authorised stay of 90 days within any period of 180 days). This calculation method is time-consuming and difficult, particularly for frequent travellers. In addition, maintaining the quality and security of stamps requires both resources and efforts, as they can be subject to counterfeiting and forgery.
The 2013 proposals provide for the abolishment of the stamping of passports of non-EU citizens crossing the external borders of the Schengen area. The Commission would like to gather views on the consequences of such abolition.

If stamps on passports were discontinued, would you need access to the information they currently provide (date and location of your entry into/exit from the Schengen area)? (question only for non-EU citizens)

- (●) Yes
- ( ) No
- ( ) No opinion / Not sure

* If yes, why would you need to access this information? (You may tick more than one box) (question only for non-EU citizens)

- [x] To make sure during my stay in the Schengen area that my planned return date complies with the authorised stay in the Schengen area (90 days within 180 days)
- [x] To plan my future trip(s) to the Schengen area and make sure I comply with the rules on the authorised period for a short stay (90 days within 180 days)
- [x] To prove my absence from my country of residence
- [ ] Other

* If yes, how would you prefer to have access to this information? (question only for non-EU citizens)

- ( ) From an online website
- (●) From a printed receipt given when crossing the external borders of the Schengen area
- ( ) By having it displayed on screen in the border guards booth when you cross the external borders of the Schengen area
- ( ) Other: (maximum 150 characters)

Contact

✉ HOME-SMART-BORDERS@ec.europa.eu

Key points:

It is likely that large scale biometric data losses will occur from immigration databases such as the EU EES.

The EC is recommended to establish a regime of reciprocal liability between other nations in case of loss of EU citizen data in those databases is indemnified by reciprocal liability in EU databases.

The EC must establish manufacturer liability standards so that biometric system software/hardware manufacturers are liable for biometric data loss to due software or hardware defect.

The EC should consider a Cyber-Insurance plan to indemnify EU and member states from biometric data loss events.

The Smart Borders Cost Study does not factor in the costs of a biometric data loss event.

The presence of certain types of individual's biometrics in the EES will make those a target. This includes celebrities, juveniles, high-net wealth individuals, etc.

The EES plan encourages other nations to collect biometric data as a condition of entry. The collection of EU citizen fingerprint data raises significant security problems, many of which pervert existing security models, such as the use of the fingerprint to safeguard EU passports.

In the long run, the EU non-national immigration databases will be difficult to secure.

As more and more immigration control agencies in the world collect biometric data as a condition of entry, the likelihood of a biometric data loss event (BDLE) increases. The first major biometric data loss event has occurred when the US Government lost 5.6 million classified employee ten-fingerprint files in a intrusion at the Office of Personnel Management. The long term consequences of this event are unknown, the costs are incalculable and the threats last for an individual's lifetime since biometrics are lifelong.

This event shows how biometrics can create new security issues which transcend the original problems they were intended to solve.

More biometric data loss events are likely and need to be assumed in all new large scale biometric database implementations.

Given that the immigration control agency databases do not contain biometric data of their own citizens, countries have a low incentive to protect the data to the best of their ability.

One solution to these issues is to create a system of **reciprocal liability** between nations, such that the liability owed to a biometric data subject in the event of loss would be reciprocated by the other state.

So for instance, the EC could enter into an agreement with Japan, such that Japan would pay a liability of $50,000 per EU citizen biometric data loss, and the EU would reciprocate for any Japanese citizen whose biometric data is lost from the EU EES system.

This would help, in some way, secure EU citizen data which is not secured by any other means today. The above referenced OPM biometric data loss event was of highly sensitive US employee data. We would assume that the US protects EU citizen data with less urgency.

During this consultation process the EC is highly encouraged to discuss **Cyber-insurance** policies in order to indemnify the EES database. The cyber-Insurance underwriting process will allow the various stakeholders to understand how much a biometric data loss event may cost an individual biometric data subject, the risk of such an event, as well as 3rd party management of that risk through cyber-insurance premiums and underwriting.

A non-EU national traveling into the EU should be aware of how much liability coverage is provided to them in case of biometric data loss from the EES database.

The EC needs to establish protocols to ensure that **manufacturer liability** is included in the contracts/tenders for the EES system. Manufacturer liability would obviously cover any manufacturer defects in software or hardware which would cause a biometric data loss event.

1.) Member states and their citizens should not be financially responsible for a biometric data loss event when it is due to manufacturer negligence or error.

2.) Non-EU nationals should not be responsible for biometric data loss when it isn't their fault.

3.) EU citizens whose biometrics are in another nation's database should enjoy manufacturer liability in case of biometric data loss.

4.) Manufacturer liability will help increase security overall, because at this point in time many key security decisions are made by manufacturers who have no stake in the outcome (or, worse, sell new security solutions when their previous security solutions fail.)

Questions for the EC to consider:

1.) When a liability reciprocity agreement is lacking, will there be a default liability available, or none at all?

1b.) What about situations in which a reciprocity agreement is lacking but the legal system of the other nation would afford some type of general liability/manufacturer liability anyway?

2.) Would the EC consider different liability levels for different citizens, given their age (under-18/over-18) wealth status (VIPs, VVIPS) and citizenship (degree of biometric system dependence in that nation, cost of doing business in that nation)?

3.) Should the EC not establish any minimum liability for a biometric data loss event, non-EU nationals should be aware of this so they may contract with third party private insurance providers if they desire.

4.) Does a reciprocal agreement require that the EC monitor another nation's biometric data base security, so that the EC can warn EU nationals in case of security problems with another nation's biometric database?

Please keep in mind, the current EES regulation does not include the financial impact of a biometric data loss event. This event is possible within the timeframe of the financial impact analysis in section 3. The financial impact of a biometric data loss event will rise with time (thanks to higher use of biometrics in a variety of applications, improvements in biometric hardware, rising incentives for fooling biometric hardware.)

Consider this improvement in biometric hardware: When we consider the idea of fingerprint scanning we think of it in terms of fingerprints being pressed onto a scanner. However, as early as 2011 scanners were developed which could read fingerprints from a distance of 6.5 feet. Such technology will make surreptitious fingerprint scanning much easier for rogue states/organizations. As that technology gets better, individuals who have lost biometric data or individuals considering the risks of enrolling into a biometric database such as EES will have to consider security problems more carefully.

The EC needs to recognize that liability in case of a biometric loss of EU citizens data is important enough that ensuring reciprocal liability is essential for EU citizen security.

This proposal brings with it the security issues that it encourages other nations to collect EU citizen biometric data as a condition of entry.

These other nations may:

*have lax security for the databases holding EU citizen biometric data
*have substantial diplomatic issues with the EU or EU member states
*freely share EU citizen biometric data with rogue states or organizations
*be subject to high speed regime change or terrorism in which case EU citizen biometric data may quickly fall into the wrong hands
*become involved in a cyberwar in which biometric databases are attacked

Obviously a policy which encourages other nations to collect EU citizen biometric data is at odds with other policies. For instance, Regulation (EC) 2252/2004 has the fingerprint used as a biometric identifier to protect the EU passport. A second policy (such as this one) which encourages nations which have security conflicts with the EU to collect EU citizen fingerprints is contradictory and problematic.

This matter needs to be urgently reviewed since it is more likely that EU citizen biometric data will be lost in another nation's immigration database than the EU losing such data. So the reciprocity agreements in place in regards to the proposed EES system will help indemnify EU citizens and protect their security.

However in the long run, the EU non-national immigration databases will be difficult to secure.

High value non-EU nationals' (wealthy individuals, celebrities, non-diplomatic politicians, etc) biometric data will be in the database and that will be a target for a variety of countries and rogue organizations.

Scenarios

A variety of scenarios are presented for the Commission's consideration.

1.) A biometric data loss event which results in the loss of the fingerprints of 50,000 non-EU citizens.

2.) A biometric data loss event which results in the loss of the fingerprints of 100,000 non-EU citizens.

3.) A biometric data loss event which results in the loss of the fingerprints of 25,000 high profile non-EU citizens (very high net wealth individuals, celebrities, non-diplomatic public officials, individuals under age 18, etc.)

4.) A biometric data loss event which results in the loss of 2,000,000 records pertaining to the citizens of only one nation.

5.) A biometric data loss event which results in the loss of fingerprints, photographs and passport details of the entirety of the EES database of 100+ million records.

As the EC considers the above scenarios, the following needs to be addressed:

1.) Assuming a variety of manufacturer liability scenarios for the above biometric data loss events (such as 100% manufacturer liability, 50%, 0%) what would be the cost burden to the EC?

2.) How will the EC mitigate a biometric data loss event for non-EU nationals?

Biometric manufacturer sales to certain nations:

Though biometric scanning and storage equipment are not *yet* part of the The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, the EC is strongly urged to require that the contract bid winner(s) for the Smart Borders Package do not supply biometric scanning/storage equipment to nations with a history civil rights violations. This would be good for the security and civil rights of both EU and non-EU citizens.

Biometric scanning/storage devices are arguably a dual-use good and may feature in future control list revisions.

Issues regarding consent

Unambiguous, informed consent is the EU standard. This would presumably require that airlines inform non nationals at the time of ticket booking that biometrics would be collected, the rules under which that occurs, and the risks (such as biometric data loss and the liability indemnifications (or lack thereof) where applicable.

Per EC request, this document was posted online and a link to it submitted in the electronic survey for the Public Consultation on the Smart Borders Package.