CEPS Policy brief
No. 154 • March 2008

The Commission's New Border Package

Does it take us one step closer to a 'cyber-fortress Europe'?

Elspeth Guild, Sergio Carrera and Florian Geyer

The European Commission presented a new 'Border Package' on 13 February 2008, setting out its vision of how to foster the further management of the EU's external border. Billed in a Commission press release as a "comprehensive vision for an integrated European border management system for the 21st century", one of the key elements of this package[1] is a Communication aimed at establishing an EU entry/exit system registering the movement of specific categories of third country nationals[2] at the external borders of the EU.[3] This Communication furthermore recommends the setting up of an Automated Border Control System enabling the automated verification of a traveller's identity (for both citizens and non-EU citizens alike), based on biometric technology as well as an Electronic Travel Authorisation System – abbreviated to ETA[4] – which would oblige non-EU travellers to provide personal data for a pre-departure online check.

These security tools and techniques imply:

1. The setting up of a new European-wide database containing specific information on certain categories of non EU-nationals;
2. Interoperability of the database with other already existing and planned EU databases and biometric systems; and
3. The systematic checking of everyone entering and leaving the EU for at least three categories of persons:
   - third country nationals who have visas containing biometric data, which will be checked at the border,
   - third country nationals who do not need visas for a short stay in the EU whose biometric data will be taken at the border and
   - citizens of the EU whose biometric data will be incorporated into their passports which will be swiped on entry and exit.

The proposal raises several important questions: Is it feasible and necessary? Does it have a legitimate objective? Is it consistent with EU data protection rules, fundamental rights and the principle of proportionality? Is there any appreciable added value of such a system, bearing in mind its many costs?

1. An outline of the proposed measures

The main group of people targeted by the **EU entry/exit system** are third country nationals admitted for a short-stay of up to three months, regardless of whether they require a visa to enter the EU or not. Only holders of a local border permit, national long-stay visa or a residence

[1] A Communication on the evaluation and further development of the EU's external border agency Frontex as well as a Communication examining the establishment of a satellite-based border surveillance system (Eurosur) are the other elements of the package.

[2] All non-EU citizens.

[3] Commission Communication, Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008.

[4] Whether this commonly used abbreviation was chosen accidentally remains unclear.

Elspeth Guild is Senior Research Fellow in the Justice and Home Affairs Unit of CEPS, of which Sergio Carrera is Head of Section and Research Fellow and Florian Geyer Research Fellow. This paper falls within the scope of the CHALLENGE project – *the Changing Landscape of Liberty and Security*, funded by the Sixth EU Framework Programme of DG Research, European Commission (see www.libertysecurity.org).

permit as well as third country nationals who are exempted from stamping (e.g. pilots, seamen of cruise ships, diplomats, etc.) will not be registered in the system. The database will include data on the time and place of entry, the length of stay authorised, the transmission of automated alerts to the competent authorities as well as biometric data of the people registered.

The Communication furthermore suggests that those falling within the category of 'low-risk travellers' could be awarded a **Registered Traveller Status** and be subject to an automated regime of control. The criteria for labelling someone as 'low-risk' would include, in the words of the Communication, factors such as a reliable travel history (mainly no previous overstays), evidence of sufficient financial means, holding a biometric passport containing fingerprints, successful visa applications, etc. However, to become a low-risk traveller, the third country national needs to have previously travelled to the EU and stayed for a while. There is no obvious way in which a third country national who has never been to the EU could obtain that status.

The Communication then recommends exploring the possibilities for setting up a **European Electronic Travel Authorisation** (ETA) system that will request third country nationals to make an electronic application supplying personal and passport data before departure, which would be a condition for their entry into the EU. A third country traveller would only be allowed to enter when the on-line check against certain databases reveals no contrary indicator.

However, it is not only foreigners who are expected to 'profit' from the new era of 'border control by technology' liberated from any border guard interaction. The **Automated Border Control System** will also apply to EU citizens entering and leaving the external border. EU citizens will have to have an e-passport containing biometric data (expected to be in place by 2019 for two biometric identifiers) which the system can read and check against EU and national databases. The Commission's impact assessment reads as follows in this respect: "The primary requirement of an Automated Border Control process for EU citizens is to automatically verify the claim of EU citizenship through the authentication of the travel document and traveller".[5] Undoubtedly, a remarkable vision for the 21st century: machines at border crossing points will henceforth determine whether an EU citizen's claim of his EU citizenship is verified!

2. A critical assessment

As regards the collection of personal data, European databases, whether public or private, are subject to laws. These laws, at national and EU level, have been designed to protect the individual against misuse of his or her data. A number of principles are at the heart of this system, as contained for instance in the Council data protection Directive 95/46[6] and in Article 8 of the Charter of Fundamental Rights of the Union.[7] Among the most important of the principles regulating European databases in the scope of the EC legal regime are the general principles of EC law, and particularly those of proportionality and fundamental rights. Whenever a public authority at EU or national level plans the development and implementation of a new database containing personal data of individuals, and therefore potentially affecting the right to data protection, the following questions must be addressed: What are the goals pursued by this database? Do they correspond to a real social need that is legitimate and goes no further than what is necessary to achieve the purported objective? What are the mechanisms of protection offered to the fundamental rights of the targeted individual?

A certain tension arises between the Commission's vision and recommendations and the tests of proportionality and fundamental rights. This tension becomes evident when looking at the objectives pursued by the proposal and their repercussions on liberty, which may be summarised as follows:

First, it is claimed that this EU system would facilitate the entry of *bona fide* travellers. However, as far as we have been able to ascertain, *bona fide* travellers do not currently encounter any obstacles to entry that such a system might address. The development of EC Visa Facilitation Agreements with most of the countries in the European region, including for instance Russia, are already designed to facilitate the entry of *bona fide* third country nationals, and even these agreements, which cut the red tape,

[5] Commission Staff Working Document, Accompanying document to the Commission Communication, Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008, p. 55.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995. Article 1.1 states that "*1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*".

[7] Article 8.1 stipulates that "*Everyone has the right to the protection of personal data concerning him or her*".

have been subject to criticism. A measure that would increase red tape and the risk of mistake, error and malice is unlikely to facilitate entry of *bona fide* travellers.

Second, very few third country nationals issued with visas face any difficulty at the EU external border, and this proposal addresses first and foremost third country nationals who require visas to come to the EU. If EU visa officers in the countries of origin do their job properly then they command the respect of their counterparts at the external frontier. The introduction of another system of checks and the creation of a new database are likely to increase suspicion between visa officers abroad and border guards at the external frontier. There will no longer be the presumption that everyone is doing their job correctly but rather the risk of introducing a culture where every official is checking and doubting the work of his or her colleagues, all directed towards excluding third country nationals.

Third, the proposal also suggests that such a system would assist in determining how many third country nationals overstay their visas each year. This objective, however, is statistical in nature and would be addressed with much less expense and intrusion into the lives and rights of individuals by clever proposals from statisticians on how to capture data. Quite rightly, the proposal does not suggest that the system would have any actual consequence for third country nationals overstaying their visas since finding them is quite another matter from simply registering who entered and who left into a database. And this leaves aside the further complications of dual nationals, third country national family members of EU nationals, third country nationals arriving on tourist visas to the EU but have a right of residence, asylum seekers who are lawfully in the EU while their application for protection is under consideration and all those other cases where an individual's status changes while s/he is in the EU. The certainty of miscalculation, erring on the side of over-counting, would only create anxiety in a public already concerned about the adequacy of immigration controls at the external borders.

Fourth, not one of the above considerations addresses the rights of a data subject to privacy and protection. Not only is the proportionality of the initiative most acutely in question here, but it also open questions such as the length of time for which the data would be retained, the duty to limit who has access to that data and the right to correction of the data remain unanswered. In fact, what would be the mechanisms and guarantees at the disposal of the targeted third country national to resist any possible disproportionate and intrusive practice in the scope of the EU entry/exit system? This question should also trouble EU citizens as they are intended to be subject to the Automated Border Control System. Although it is stated that their data would not be stored, the automated gate system would nevertheless "read and extract the information from the travel document, capturing biometrics and performing the verification to enable entry or exit, as a well as random checks of the SIS and national databases."[8] What kind of national databases is not further specified and in the age of 'interoperability' anything might be possible one day, including national tax authorities, social welfare offices, etc.

It is surprising that the Communication attempts to present the establishment of these security tools "for the benefit of" *bona fide* travellers, who would then experience an automated and faster processing at EU external borders. There appears to be an untested belief shared by some EU officials that this logic of acceleration in people's lives should take precedence over its implications for fundamental rights, and particularly that of data protection. Also, the Europeanisation processes are fostering the belief that technology represents the solution to any imagined threat to security, without duly considering that it may end up creating more insecurity in terms of data protection.[9] Rapidity is often difficult to reconcile with liberty, as judges well know. The Commission should better acknowledge the fact that the use of technology primarily aims at increasing and dispersing mobility control, not making the lives of individuals easier. This strategy leads to intrusive practices into individuals' lives. The EU entry/exit system may confront the EU and its member states with serious difficulties with respect to the principles of liberty, fundamental freedoms and the rule of law as stipulated in Article 6 Treaty on European Union.

Fifth, although the question of feasibility might be one for the technical experts to answer in the first place, it is worth imagining the dimensions required to realise the proposal. The logistics of getting every border post in 28 countries (assuming Ireland and the UK are out but Denmark, Iceland, Norway and Switzerland will be in via their Schengen participation) tooled up and connected to such a system – which is a precondition for its working – are gigantic. Making sure that the system and its interlinkages

[8] Commission Communication, Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008, p. 6.

[9] On this latter aspect, see D. Bigo and S. Carrera, "From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU", CEPS Commentary, April 2004.

with all the other EU databases are secure will be even more challenging. At the rate at which personal information is currently misplaced or corrupted by administrations around the EU, it will not be surprising if experts have differing views on the feasibility of such a project.

Sixth, in light of systems and databases already in place or soon to be active, one wonders whether this new package is actually necessary; this in particular when measuring it against its possible negative trajectories. All third country nationals who need a visa to enter EU territory will already be registered in the soon-to-be Visa Information System (VIS). Name, address, occupation as well as visa-application history, biometric photograph and fingerprints will be stored and available for immigration and law enforcement purposes. Next, we have the database EURODAC to gather and store data on asylum seekers and persons apprehended in connection with irregular crossings of external borders. On top of that, EURODAC is also available to run searches on third-country nationals found illegally present in a member state, which includes 'visa over-stayers'. Then there is the Schengen Information System (SIS), which contains nearly a million entries on wanted persons, the majority of whom are persons who should be denied entry to the Schengen area. SIS (as well as national databases in member states) are consulted not only during the visa application procedure but again at the border post itself. At EU borders, the Schengen Borders Code requires EU border guards to conduct a "thorough check" of third country nationals. This implies a check to determine the purpose of stay as well as the existence of sufficient means of subsistence. A stamp has to be affixed in the traveller's document stating the date of entry. Additional checks of the person, including yet another search in SIS and national databases, are possible when leaving EU territory.

This, however, is not all. Before arriving at EU borders, Directive 2004/82/EC[10] requires air carriers to supply EU border authorities in advance with an extensive set of personal data of all travellers on incoming flights allowing the authorities to perform security checks even before travellers physically appear at the border post. Surprisingly, this Directive is not even mentioned in the Communication (although it has been acknowledged in the impact assessment). Finally, there is also the Commission's proposal to establish an EU Passenger Name Record (PNR) System,[11] mimicking the EU-US PNR agreement of July 2007 which itself has been much criticised by the European Parliament's LIBE Committee as well as national parliaments.[12] Even more personal data than under Directive 2004/82/EC, including payment information, seat number, travel agent, baggage information, etc., on all passengers entering or leaving EU territory by airplane should be gathered, stored, processed and analysed under this PNR scheme.

And yet, all this is not enough, the Commission argues. We are asked to believe that new measures or, as formulated by the Communication, "additional layers of security" are needed. It seems as if the Commission wants to soothe our fears and anxieties (stirred by actual and perceived threats[13]) with a bittersweet EU '*millefeuille* of security'.

3. Conclusions

The Commission's proposal is ill-considered and is likely to have substantial counterproductive effects on the ground. It is expected to create the same sort of public relations problems as do similar US measures among a travelling public that finds itself increasingly the object of state suspicion, with no concrete reason or grounds. The case of Senator Edward M. ('Ted') Kennedy who found himself on the 'no-fly list' being repeatedly detained and questioned at airports is just one, but a very prominent example.[14]

It is by no means clear that the proposed entry/exit system will provide any useful or reliable data on overstays by third country nationals in the EU. It does not present any reasonable and proportionate objective that is discernable from the Communication and it is likely to offend a myriad of European laws and principles of data protection and use.

The EU and its institutions, as well as the member states, need to comply with the EU legal system of guarantees and protection offered to the individual at times of applying EC law and implementing the EU integrated border management strategy. The latter should position the rule of law as one of its founding premises. In fact, it is the relationship between proportionality, data protection and the new security technological systems of surveillance proposed

[10] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, p. 24.

[11] Commission proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final, 6.11.2007.

[12] See e.g. German Bundesrat, Bundesratsdrucksache 826/1/07, 4 February 2008.

[13] An account of which is provided in the European Security Strategy of 12 December 2003, entitled "A secure Europe in a better world".

[14] "Senator Kennedy flagged by no-fly list", *Washington Post*, 20 August 2004.

by the Communication that is the real challenge for a "comprehensive vision for an integrated European border management system for the 21st century".

4. Recommendations

The Commission envisages the system to be operational by 2015. However, the Communication itself is just the first step. Legislative amendments to the Schengen Border Code, the Common Consular Instructions, as well as separate decisions will be required to implement all the envisaged measures. These have so far not been proposed. In fact, the Commission committed itself to assess the presentation of concrete legislative proposals based on the discussions of its Communication, which is expected to take place in the European Parliament and the Council.[15] The Commission furthermore emphasised that the EU must remain open and accessible to others if it wants to share its values and support economic growth.[16]

In light of this commitment, we recommend the following steps:

- All involved actors should carefully and thoroughly establish whether the envisaged measures are truly necessary and proportional and live up to our vision of an open and welcoming Union that is founded on the principles of liberty, respect for human rights and the rule of law (Art. 6 TEU).
- The enhanced use of new technologies in the changing landscape of European security policies must be duly tested against its ethical implications.
- No new EU large-scale IT systems of the dimensions of SIS II and VIS should be agreed upon and established before SIS II and VIS are actually operational and have proven to be proportional, safe and reliable.
- The Commission and the private sector should seriously advance the idea of 'data protection by design'[17] and make it an obligatory element in the programming of new and existing databases.
- Finally, none of the legislative proposals required to install the Commission's new Border Package should be tabled before the Lisbon Treaty has entered into force, providing for the necessary democratic and judicial checks and balances.

[15] The Ministerial Conference on the Challenges of the EU External Border Management, to be convened by the Slovenian Presidency on 11-12 March 2008 should provide a first suitable venue for debate and reflection.

[16] Commission Communication, Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008, p. 2.

[17] See presentation by the German Federal Commissioner for Data Protection, Peter Schaar, "Should we switch off the internet?", at the 27th International Conference of Data Protection and Privacy Commissioners, 14-16 September 2005 (available at http://www.privacyconference2005.org/fileadmin/PDF/pschaar.pdf). This idea entails the concept that data protection elements, like purpose limitation, rules on transmission, storage time, information to the data subject, etc. are governed automatically. For example, after the legally allowed data retention period, the stored set of data would automatically be deleted from the database. Similarly an automated notification could be sent out to the individual once his/her personal data has been stored in a database.