SPEECH | 15 January 2018

Commissioner King Presents Interoperability Proposals to LIBE Committee, European Parliament, Strasbourg

Introduction

I am glad we can talk once again about our work on interoperability – closing the information gap for Europe's police and border guards. We submitted legislative proposals in December. They follow the lines I set out to you in November, and I am grateful to this Committee for all its input.

The need to act on interoperability

I believe there is **broad consensus between** Parliament, Council and Commission on the need to act in this area. Security is the number one priority in the Institutions' joint declaration of last month, and this proposal is the first piece of legislation on the list.

This should come as no surprise, given security consistently ranks among the major concerns of Europeans.

I appreciate this Committee's readiness to discuss this high priority topic so quickly, and I will always be at your disposal to hold more detailed discussions as necessary.

Those on the front line should have the information they need to do their

jobs and keep our citizens safe. And our information systems can and should help them do so.

Police and border guards shouldn't face blind spots. Member States tell us for example there are too many people, including criminals, registered in EU databases under false identities. That is not acceptable.

National authorities should have the information they need, when and where they need it, with all the safeguards offered by our fundamental rights framework. And our information systems should provide them with data that is timely, complete, accurate and reliable.

By closing down the gaps terrorists and criminals can exploit, we can cut down on identity fraud, strengthening our external border and internal security.

The question now is how to turn this general consensus on the objectives into practical action: to agree swiftly, and then implement, a legislative text that can make a real and significant operational difference for those on the ground.

Legislative proposals on interoperability

Legally speaking, I should say, our proposal of December is in fact two proposals. This is because there are different levels of Member State participation in the different databases – "variable geometry" due to the participation of associated countries in Schengen, and the opt-outs of some Member States.

Of course a particular country can only benefit from databases in which it participates. Two different regulations are needed to take account of these differences and ensure they apply effectively. That said, in substance we are presenting **one comprehensive package** to address interoperability.

Interoperability components

The proposals aim to connect the dots and close the information gaps.

We need to make **best use of existing data**. When border guards or the police verify identity documents, they should get all the information they need on a single screen – as long, of course, as they have access rights to it.

So the proposals set out a **European search portal** to enable authorised users to carry out a single search and receive results from all the systems they are authorised to access, rather than searching in each system individually. Rather than having to decide which database to check, they would have a "one-stop shop", simultaneously checking against multiple systems in line with existing access rights.

In addition, a **shared biometric matching service** – a search engine - would allow users to search more efficiently and cross-match biometric data which is stored in the respective systems.

These two components would help ensure end-users have fast, systematic and controlled access to the information that they need to perform their tasks. Again, the individual access rights of each system would not change, and would have to be respected.

We also need specifically to **detect multiple identities and counter identity fraud**. So we propose a **common identity repository** grouping basic biographical and biometric information, such as names and dates of birth of non-EU citizens, so that they can be reliably identified. And, building on these systems, we propose a **multiple-identity detector** to check whether the biographical data searched for exists in multiple systems.

The multiple-identify detector is not a system in itself, but an add-on to existing systems. Authorised officers would get an automatic warning

about a potentially fraudulent identity every time they check someone against a database. So, when there are multiple identities linked to the same set of biometric data, we can detect that, combatting identity fraud.

I would remind you all that a number of perpetrators of recent terrorist attacks have hidden behind multiple identities.

Taken together, these four interoperability components would mean quicker, fuller and more **systematic** access to the data that police, migration officials and border guards need to do their jobs.

Operational innovations

Beyond these technical components, I'd like to highlight two important aspects of our proposals relating to the **processes** and **procedures** for access to databases. When we last discussed interoperability in November, I mentioned two shortcomings we had identified in consultation with Member State experts.

First, national authorities told us of the difficulties they face when trying to verify the identity of a **third-country** national within their territory. So we propose that authorised police officers should have **access to the common identity repository** to facilitate and assist the correct identification of people within the territory – with access limited to the identity information contained in the common identity repository.

This innovation would fill a large gap in the current information architecture. Searches against the common identify repository would be enabled on any person unable or unwilling to identify themselves to police during an identity check.

This would make it easier to check the identity of third-country nationals within a Member State's territory. Such checks are a major part of our work to lift internal border restrictions and get "back to Schengen". We

cannot run the risk of people disappearing into an information black hole once they are within the shared Schengen space.

Second, the High-Level Expert Group has raised concerns over the difficulties for police authorities investigating terrorism or serious crime to access border and migration databases to identify suspects or victims. We recognise this is sensitive. Police can get access. But it is very slow. We believe we can maintain data protection safeguards with a more effective approach.

So, we propose to streamline access by law enforcement authorities to our non-law enforcement systems, where they need it to prevent, investigate, detect or prosecute terrorism or serious crime. In practice, we propose to replace the current **'cascading approach'** - where you consult systems one by one, in turn - with a new **two-step approach**: first a 'data presence check' against all relevant systems. This step would not need prior authorisation, but would just confirm or deny, yes or no, whether the given person was on any given system. As a second step, the authorities could then consult those systems that contain data on the person in question — a request which would have to respect fully the conditions and procedures set out in existing laws.

Without changing access rights, this new approach would make the authorities' work easier, and more efficient. I would maintain that it is also more proportionate, because it saves them making excessive requests into systems that in reality do not hold any relevant data.

Both of these proposed operational innovations – identity checks within the territory and streamlining the rules for law enforcement access – are the result of careful analysis in our impact assessment. The changes we propose to rules and procedures are necessary, proportionate and in full compliance with fundamental rights.

Fundamental Rights

Our extensive consultation included Member States, but also the Fundamental Rights Agency, the European Data Protection Supervisor, the Counter-Terrorism Coordinator, Europol, Frontex, the Asylum Support Office, and eu-LISA, which develops and maintains the relevant systems.

We have endeavoured to take account of the many issues and views raised – including on practical implementation; costs and timing; necessity and proportionality; and, most importantly, fundamental rights and data protection.

Let me focus on that last, crucial, issue. Personal data protection is a fundamental right. Our proposal is fully in line with the Charter of Fundamental Rights, the General Data Protection Regulation and all other relevant EU law. Any implications for data protection would be proportionate, pursuing a legitimate objective, and balanced against other rights and freedoms.

In particular: we are not proposing to collect new data, and we are not putting all data in one big pool. Existing access rules continue to apply – and indeed will in some cases become more streamlined and proportionate.

I read with interest the comments of Michael O'Flaherty, the Director of the Fundamental Rights Agency to the Terrorism Committee, last week. I know he stressed the points about purpose limitation, and the need to ensure data held is accurate. I agree with both his points: and these are indeed exactly what our proposal sets out to achieve.

Conclusion

I recognise that the issues we are dealing with here are very sensitive. Some aspects of these proposals are complicated and complex. They deserve thorough discussion and scrutiny. But I know that you will also be mindful of the proposal's operational importance, and political priority.

I hope we can make rapid progress with the scrutiny of this proposal in Libe, and in Council discussions with the Bulgarian Presidency.

The Commission stands ready to support you in any way we can.

We need to get this right. At the same time, I'm conscious that If you asked the man or woman on the street, they'd probably expect that many of the things we propose were happening already. But they are not. Or they are technically possible, but so awkward or lengthy that they aren't done in practice. That needs to change.

Interoperability is not about creating 'big brother". It's not about creating an enormous database where everything is interconnected.

The approach would not lead to the interconnectivity of all the individual systems. They would only share information on core identity and fingerprints, to ensure that an individual cannot be registered under more than one identity and to enable the correct identification of third-country nationals in the territory of the Member States.

The new functionalities would build on existing EU systems that would keep their limitation rules. There would be no new categories collected for the purpose of interoperability. Interoperability would use data already stored in the EU systems in accordance with the rules described in their respective legal basis.

This is not about collecting more and more new data. It is about a targeted and intelligent way of using existing information held in our systems to the best effect.

I think we have a real opportunity to help make Europe safer and more secure, while safeguarding and strengthening fundamental rights. Together I hope we can grasp that opportunity.

Thank you.