Statewatch Analysis

Implementing the "principle of availability":
The European Criminal Records Information System
The European Police Records Index System
The Information Exchange Platform for Law Enforcement Authorities

Chris Jones

Contents

Executive Summary

Co-operation between the police and judicial authorities of the European Union's Member States has increased significantly in the last decade. Three recent developments include the establishment of the European Criminal Records Information System (the ECRIS), the development of a European Police Records Index System (EPRIS) and proposals for an Information Exchange Platform for Law Enforcement Authorities (IXP). This analysis covers all three, and finds a number of issues of major concern.

The European Criminal Records Information System

The ECRIS is intended to permit the exchange of information extracted from criminal records between Member States' judicial authorities. The primary intention of this is to ensure that individual's prior convictions can be taken into account if they face new criminal proceedings in a different Member State.

However, the desire for a swift and systematic exchange of information has led to the development of a highly problematic system. It is marked by serious gaps in data protection, a reliance on potentially untrustworthy automated translation, and a significant lack of oversight.

Furthermore, the scope of the system has expanded beyond the terms permitted by the relevant legislation. While the legal basis for the ECRIS permits the exchange of information on criminal convictions, guidance being developed for users of the system states that non-criminal rulings, such as those from administrative or civil courts, may also be exchanged.

The result is a system that permits the widespread exchange of highly sensitive information, with a significant lack of safeguards and the ability for this information to be used for a variety of purposes beyond criminal proceedings.

The European Police Records Index System

The EPRIS is currently being developed by Europol and a number of Member States, and is intended to provide police forces with the ability to search each others' records databases, in order to find out if and where information and intelligence on individuals can be found. The insistence of the Commission and a small group of states for its development has been already been questioned, partly due to concerns for the potential establishment of an EU-wide police database. Greater scrutiny of this measure is urgent.

The Information Exchange Platform for Law Enforcement Authorities

The IXP is the most recent of the three developments, and proposes to centralise access to all the EU's law enforcement information exchange instruments. Its development is still in the early stages, yet a suggestion to extend access to the European Union's bureaucracies – including the General Secretariat of the Council - demonstrates the potential for an unprecedented shift in the way that information is accessed, and to whom it is available. As with the EPRIS, greater knowledge and scrutiny of the proposed system is vital.

All three systems demonstrate that attempts to permit law enforcement agencies to function inside the EU's borderless 'Area of Freedom, Security and Justice' frequently take place at the expense of the individual rights that the European Union is supposedly founded upon. A significant reassessment of the approach taken by the Council and the Commission to law enforcement cooperation is necessary, as well as the necessity of greater respect for and protection of fundamental rights at the European Union level.

1. Introduction

This analysis is focused on a number of systems designed to increase the exchange of information between police and judicial authorities in European Union (EU) Member States: the European Criminal Records Information System, the European Police Records Index System, and the Information Exchange Platform for Law Enforcement Authorities. All three systems stem from demands for a greater degree of information exchange and co-operation between the law enforcement authorities of EU Member States in their attempts to turn the EU into an internally borderless "Area of Freedom, Security and Justice".

The analysis begins by looking at the principles of availability and mutual recognition, which for in the last decade have come to play an increasingly prominent role in the formulation of EU policy in the area of Justice and Home Affairs (JHA). They serve as the ideological basis for the ongoing proliferation of systems designed to assist in the cross-border exchange of information for the purposes of law enforcement. However, they also frequently lead to situations in which fundamental rights protections may be bypassed or weakened.

Following this is an examination of the European Criminal Records Information System. While there are legitimate reasons to enhance the exchange of information extracted from criminal records between the authorities of the Member States of the EU, there a wide number of problems with the system. While its roots ostensibly lie in the need to exchange

information on terrorism and serious crime, the relevant legislation permits the exchange of information on convictions for all crimes. This already-expansive scope is now being extended further to allow for the exchange of information decisions made by administrative and civil courts – in fact, any "competent authority". An examination of the scope and functioning of the system is accompanied by an analysis of the many data protection concerns that arise from the legislation establishing the system. The numerous gaps and loopholes could have been avoided had the Commission and the Council incorporated the many recommendations made to them by the European Parliament, the European Data Protection Supervisor and civil society organisations.

The European Police Records Index System is a more recent development, and one in which various interested parties have invested significant effort. The idea of the system is to allow police officers to search a system interconnecting police forces' databases. Using a "hit/no hit" system, the response to their search will tell them whether another Member State's police force holds information about a certain individual. Such a proposal raises very serious concerns with regard to the growing transnational power of the EU's police forces, and raises serious data protection concerns. Given that current discussions are being undertaken by the Working Party on Information Exchange and Data Protection – where data protection is discussed not as a guiding principle, but "as the need arises" [1] – it is urgent that wider and more critical scrutiny is given to the development of the system. The potential for the development of a Europe-wide police database has already led to concern from a number of Member States.

Finally, there is a brief examination of an even more recent proposal - the Information Exchange Platform for Law Enforcement Authorities (the IXP). The IXP would provide a single point of access to all law enforcement information exchange instruments in the EU. As with the ECRIS and the EPRIS, data protection concerns are paramount, as is the proposed scope of the system. Providing yet another example of the European Union's incessant drive to increase the availability and accessibility of information to and for law enforcement authorities, a current proposal for the IXP would permit access to the system not just to police forces and judicial bodies, but also a number of Directorate-Generals of the European Commission, and the General Secretariat of the Council.

The common thread linking these systems is the desire to increase the ability of law enforcement authorities to operate more effectively across the Member States of the European Union whose territory comprises the "Area of Freedom, Security and Justice". In doing so, the EU is neglecting many of the fundamental rights that it is, under the Lisbon Treaty, now legally obliged to uphold. The ECRIS, EPRIS and IXP show that the desire for greater security within the EU is driving the development of systems that may well be detrimental to the principles of freedom and justice.

---

1. Ad hoc Group on Information Exchange, *Summary of discussions*, 5858/10, 3 February 2010, p.2

2. Ideological basis

Mutual recognition

Mutual recognition was a policy originally applied in the economic field in order to allow the economies of European Union Member States to function as a single market, with goods produced in one member state being recognised as equivalent quality to those produced in another. This policy jumped from the first to the third pillar in 1999, when the Tampere European Council called for mutual recognition to become "a cornerstone of judicial co-operation in both civil and criminal matters in the Union." [2] This policy has been applied to both judicial and police matters, with the Prüm Treaty and the Swedish Framework Decision (*Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*) attempting to encourage both automated and manual information exchange between police forces. [3] Mutual recognition is intended to impel judicial and police authorities in one member state to consider a decision made by the judicial and police authorities of another member state as both trustworthy and valid. This:

> "*Removes a major obstacle to cross-border law enforcement because different national standards with regard to refugee law or criminal codes no longer obstruct judicial co-operation and extradition between Member States."* [4]

It therefore allows the judicial and police authorities in the European Union to co-operate without the respective Member States having to undertake the politically unattractive option of harmonising their laws.

The Stockholm Programme, which outlines EU Justice and Home Affairs (JHA) policy from 2010 to 2014, demonstrates that the European Council and European Commission are particularly keen on expanding the use of mutual recognition. For example, whilst proposing evaluation of the effectiveness of European Union legal instruments, the conclusion of any such evaluation is reached in the same paragraph – it "should focus on specific problems and therefore facilitate full application of the mutual recognition principle." [5] Any evaluation undertaken will not be an opportunity to consider and reflect upon how certain policies and legal instruments have worked in practice, but rather will serve to further implement mutual recognition. It is also stated that:

> *"Mutual recognition could extend to all types of judgements and decisions of a judicial nature, which may, depending on the legal system, be either criminal or administrative."*[6]

---

2. Tampere European Council 15 and 16 October 1999, *Presidency Conclusions*

3. *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*

4. Sandra Lavenex, 'Mutual recognition and the monopoly of force: limits of the single market analogy', *Journal of European Public Policy*, Vol.14, No.5 (August 2007), p.763

5. *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, 17024/09, 2 December 2009, p.7

6. *The Stockholm Programme*, p.22

Furthermore, mutual recognition should be extended:

> *"To fields that are not yet covered but essential to everyday life, e.g. succession and wills, matrimonial property rights and the property consequences of the separation of couples."* [7]

Proposals for such widespread use of mutual recognition pose problems for individual rights because of the differing effects that mutual recognition has in economic and judicial affairs. Sandra Lavenex argues that mutual recognition in judicial affairs, unlike in economic affairs:

> *"Does not expand the rights of individuals vis-à-vis the state. On the contrary, it facilitates the cross-border movement of sovereign acts exercised by states' executives and judicial organs. The relationship between the principle of mutual recognition and the balance between state and society, liberalisation and sovereignty is thus reversed... The dangers of a race to the bottom in the level of regulations thus needs to be revised in relation to the AFSJ. Instead of increasing individual freedoms in relation to the regulatory scope of government, in the AFSJ, mutual recognition boosts the transnational enforcement capacity of governmental actors."* [8]

Although the Stockholm Programme contains some measures intended to use the principle of mutual recognition to benefit citizens (e.g. through enhancing the rights of victims and defendants in legal proceedings, or through the creation of an online European e-Justice portal which will allow individuals to access information regarding their legal rights), these are far outweighed by projects intended to increase the coercive and punitive power of the state. The document is marked by its insistence on "a bit more freedom and justice and a lot more security." [9]

The principle of availability

The second idea underlying the proliferation of instruments for information exchange is the principle of availability. This is a more recent development than mutual recognition but is in many ways an extension of the idea, and can be seen as "a maximal version of mutual recognition." [10] It was established as a principle of police and judicial co-operation in the Hague Programme in 2004, and is designed to allow member state police or judicial authorities to access information held by other Member States with as few procedural and judicial obstacles as possible. As a note from the Luxembourg Council Presidency stated:

> *"The aim is obviously that as large a list of information categories as possible is exchangeable with as little effort as possible (i.e. requiring a minimum of formalities, permissions, procedures, if any)."* [11]

---

7. Ibid., p.24

8. Lavenex, 'Mutual recognition and the monopoly of force', p.765

9. Tony Bunyan, *Commission: Action Plan on the Stockholm Programme, a bit more freedom and justice and a lot more security*, Statewatch Analysis no. 95,

10. Valsamis Mitsilegas, *EU Criminal Law*. Hart: Oxford, 2009, p.257

11. Quoted in Tony Bunyan, *The "principle of availability"*, December 2006, p.2

In line with mutual recognition, all such information held by what the Member States determine to be a competent authority is to be considered of the same quality as information held by any other competent authority within the EU. By making all such information available for access by authorities in other Member States the process of cross-border cooperation is intensified. This is intended to permit the swifter application of justice, and help create a common European police and judicial culture.

The principle of availability appears by name only once in the Stockholm Programme, with the statement that there is now:

> *"An extensive toolbox for collecting, processing and sharing information between national authorities and other European players in the area of freedom, security and justice. The principle of availability will continue to give important impetus to this work."*[12]

Despite this single instance of the term itself, the influence of the idea is immediately apparent whenever the subject of information exchange is raised. Information exchange must be "improved", "developed" or "enhanced." [13] The outline of an *Information Management Strategy* even goes so far as to propose "business-driven development," defined as "a development of information exchange and its tools that is driven by law enforcement needs." Permitting law enforcement authorities to write themselves wish-lists should be anathema to a democratic society, and such a proposal sits uneasily alongside the two statements which follow it. These call for "a strong data protection regime" and "well targeted data collection, both to protect fundamental rights of citizens and avoid an information overflow for the competent authorities." [14]

According to the Stockholm Programme, one of the chief challenges in the coming years for the European Union is "to ensure respect for fundamental freedoms and integrity while guaranteeing security in Europe." [15] One aspect of this challenge is ensuring that the European Union and its Member States work to create "a Europe of law and justice." Presumably this is meant to imply law that is grounded in open, democratic decision-making and is applied equally, and justice that is impartial and fair. These ideals are sharply undermined by the already-noted fact that tools designed for information exchange are to be "driven by law enforcement needs." [16] This proposal itself is contrary to the idea that "law enforcement measures and measures to safeguard individual rights... [should] go hand in hand in the same direction." [17] Driven by the principles of availability and mutual recognition, the current needs of law enforcement authorities seem to revolve around making the maximum amount information about those with a criminal or police record

---

12. *The Stockholm Programme*, p.37
13. Ibid., pp.36, 48, 56
14. Ibid., p.38
15. Ibid., p.3
16. Ibid., p.38
17. Ibid., p.3

available for exchange through large-scale computer networks, often with little sense of proportionality or respect for the rights of individuals to privacy and data protection.

3. The European Criminal Records Information System (the ECRIS)

Basic principles

The ECRIS is a system designed to provide competent authorities from one European Union member state with access to information from the criminal records of individuals from another member state. Its stated purpose is to facilitate the exchange of information from criminal records, so that individuals' previous convictions can be taken into account if they become involved in new criminal proceedings. It is currently estimated that 100,000 messages per month will be exchanged via the system. [18]

As with all the systems established to enhance mutual recognition in the judicial field, the ECRIS "facilitates the cross-border movement of sovereign acts exercised by states' executive and judicial organs." [19] In this case those acts are ones which result in an individual being arrested, tried, convicted and given a criminal record. This is likely to be extended to allow "the exchange of information on supervision measures," [20] and documentation indicates that the definition of conviction provided in the legislation is being stretched to cover non-criminal rulings that are entered into an individual's criminal record. It is significant that there is no common European definition of what constitutes a criminal record. Furthermore, despite the original purpose being to exchange information for use in criminal proceedings (specifically at the pre-trial, trial, and sentencing stages), use of the system has been expanded to allow requests from "bodies authorised to vet persons for sensitive employment or firearms ownership." [21]

Every member state is supposed to be using the ECRIS to exchange information from individuals' criminal records by April 2012. In 2012 there will also be a legislative proposal on an "ECRIS-TCN" system (European Criminal Records Information System – Third Country Nationals). [22] This would move the ECRIS beyond its current remit, which covers only EU citizens, and may well see the introduction of a centralised European database to hold information on convicted third country nationals.

Development of the system

The exchange of information extracted from criminal records amongst judicial and other authorities has a lengthy history in Europe. The 1959 *Council of Europe Convention on*

---

18. European Commission, *Background information related to the strategy for expanding and developing the Internal Market Information System ('IMI')*, SEC(2011) 206, 22 February 2011, p.13

19. Sandra Lavenex, 'Mutual recognition and the monopoly of force', p.765

20. *The Stockholm Programme*, p.40

21. European Commission, *Overview of information management in the area of freedom, security and justice*, 12579/10, 26 July 2010, p.12

22. European Commission, *Annexes to the Commission Work Programme 2011, Volume II*, COM(2010) 623, 03 November 2010, p.25

Mutual Assistance in Criminal Matters laid a multilateral foundation for the exchange of such information. By the 1990s, it was clear that judicial and law enforcement cooperation in the EU "lagged behind political and economic cooperation." [23] The Treaty of Amsterdam committed the Member States to enhance mutual assistance in criminal matters as part of the programme of developing an Area of Freedom, Security and Justice. Amsterdam, which entered into force in 1999, was followed in 2000 by the *Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*.

As noted earlier, it was decided around this time that principle of mutual recognition should be extended to police and judicial cooperation, following the Tampere European council of 1999. The *Mutual Recognition Plan* that followed this in 2000 envisaged a "two-step approach" towards improving the accessibility of individuals' criminal records to authorities in different Member States:

> *"[T]he first step would be limited to developing common European multi-language forms that could be used to request information on existing criminal records…. In a second stage, a true European Criminal Registry should be created."* [24]

A subsequent study commissioned by the EU recommended a "network of national registers using a common index system of labels for common criminal offences," [25] rather than any sort of centralised database. The ECRIS is based on this type of system, despite the ongoing desire from the Council to establish a "European register on convictions and disqualifications," as stated in the *Declaration on Combating Terrorism* that followed the 2004 Madrid bombings. [26]

In 2005 a *White Paper on exchanges of information on convictions and the effect of such convictions in the European Union* was published by the Commission, [27] and later in the year a *Proposal for a Council framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States* appeared. *Council Framework Decision 2008/675/JHA on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings* followed. The two pieces of legislation that led to the creation of the ECRIS are *Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States*, and the accompanying *Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA*, which itself stemmed from a 2008 proposal. Both pieces of legislation are problematic in a number of ways, most notably with regard to data

---

23. James B. Jacobs and Dimitra Blitsa, 'Major "minor" Progress under the Third Pillar: EU Institution Building in the Sharing of Criminal Record Information', 2008, p.113

24. European Commission, *Mutual Recognition of Final Decisions in Criminal Matters* COM(2000) 495 final, 26 July 2000, p.7

25. Jacobs and Blitsa, 'Major "minor" progress', p.5

26. Council of the European Union, *Declaration on Combating Terrorism*, 25 March 2004, p.5

27. European Commission, *White Paper on exchanges of information on convictions and the effect of such convictions in the European Union*, COM(2005) 10 final, 25 January 2005

protection principles. However, the expansive scope of the system is also a cause for concern.

Scope of the system

As noted, there is a long history of moves towards the more systematic exchange of information from criminal records. Recent justifications for this exchange have been based on terrorism and serious crime. The preamble of *Council Decision 2009/316/JHA* states that the idea for such a system was "initially prioritised in the *European Council Declaration on Combating Terrorism of 25 and 26 March 2004*." Preliminary documentation for the ECRIS is however more revealing than the legislation itself, making reference to a Belgian proposal of November 2004 on "mutual recognition of disqualification from working with children as a result of convictions for child pornography offences." [28] Sex offenders' criminal records were also mentioned as a justification for the improved exchange of information on convictions in the Hague Programme's section on mutual recognition. [29]

Preliminary documentation for the *Framework Decision on taking account of convictions in Member States of the EU in the course of new criminal proceedings* also mentions the need to include road traffic offences in the list of relevant crimes. Such offences are "a category where it is particularly worth tackling the problem of repeat offending." [30] The EU's *Overview of information management in the area of freedom, security and justice* places the roots of the ECRIS firmly in the 2004 Belgian initiative, and does not mention the other motivations. [31] While convictions for sex offences are clearly very serious matters on which information should be exchanged with stringent safeguards between Member States when necessary, this does not presuppose a need to exchange information on all offences. Nevertheless, this is precisely what is to be attempted, regardless of how minor a conviction an individual holds. Furthermore, the development of a manual intended to provide guidance to authorities who will be using the system has led to a widening of the scope of information exchange via the ECRIS.

Article 2(a) of *Council Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States* contains a definition of "conviction", which is:

> *"Any final decision of a criminal court against a natural person in respect of a criminal offence, to the extent these decisions are entered in the criminal record of the convicting Member State."*

This limits the information available for exchange in a relatively strict way, although there

---

28. European Commission, *White Paper*, p.5-6

29. Council of the European Union, *The Hague Programme: strengthening freedom, security and justice in the European Union*, 2005/C 53/01, 13 December 2004, p.29

30. European Commission, *Proposal for a Council Framework Decision on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings*, COM(2005) 91 final, 17 March 2005, p.6

31. *Overview of information management in the area of freedom, security and justice*, p.12

will be limitations depending on how Member States organise their criminal records. The Commission's 2005 *White Paper* states that:

> *"Some [national criminal record] registers contain all convictions; others merely indicate the most serious offences. Some record convictions against legal persons; others do not. Some are limited to final judgments (res judicata); others record, at least temporarily, judgments that are subject to appeal. Some registers also contain a section devoted to ongoing proceedings and certain acquittals or dismissals, in particular on the grounds of mental incapacity. In some Member States only judgments given by criminal courts are recorded. In other cases, decisions by administrative authorities or commercial courts, for example to impose disciplinary penalties or to remove the right to exercise certain occupations, are also included. Information on methods of enforcing sentences also varies."* [32]

Thus, it may be the case that due to the way in which a Member State organises its criminal records, information on an individual's criminal conviction(s) will not be available for exchange. It was remarked by one author that the 2008 proposal to establish the ECRIS was "premature", precisely because of the "diversity in what constitutes a 'criminal conviction' and what is included in a 'criminal record' in national systems." [33]

Nothing, it seems, has been done to address this diversity, but this was in some ways countered by the relatively limited definition provided in *Decision 2009/315/JHA.* However, a document containing a draft version of the proposed manual for those who will be using the system contains the statement that the Article 2(a) definition "covers also non-criminal rulings." It goes on to broaden the scope even further:

> *"The term "decision" is more general than "conviction" defined above. It is understood as any final decision from a* ***competent authority****, to the extent that these are recorded in the criminal records register of the convicting Member State."* [34] (emphasis in original)

There is no justification for this expansion. While there are many faults with the ECRIS, the definition contained in Article 2(a) is clear. The system has moved beyond the exchange of information related to convictions for terrorism and serious crime, to the exchange of information related to convictions for all crimes. Now the exchange of yet more information – potentially that stemming from administrative or civil courts – has been approved, with no formal procedure or consultation.

How the ECRIS functions

There are two key components to the ECRIS. In the words of the Council:

> *"The ECRIS is a decentralised information technology system based on the criminal records databases in each Member State. It is composed of the following elements:*

---

32. European Commission, *White Paper*, p.3

33. Mitsilegas, *EU Criminal Law*, p.251

34. Presidency, *Draft Manual for practitioners – ECRIS – Request for contributions*, 9300/11, 19 April 2011, p.22

(a) an interconnection software built in compliance with a common set of protocols enabling the exchange of information between Member States' criminal records databases;
(b) a common communication infrastructure that provides an encrypted network."[35]

'Common set of protocols'

The "common set of protocols enabling the exchange of information" comes in the form of a series of "tables", where information can be automatically translated from one language to another through the use of machine-readable codes. For example, "offences against migration law" are attached to code 2300 00, with 2301 00 ("unauthorised entry or residence") as a sub-category. The table of categories of offences is certainly extensive, ranging from "unintentional environmental offences" to genocide and war crimes. The tables are supposed to cover the entire criminal code of each member state of the EU. [36]

The use of automatic translation in relation to something as sensitive as an individual's criminal record poses potentially enormous problems. In this respect it is important to note that the legislation establishing the ECRIS (*Council Decision 2009/316/JHA*) fails to differentiate between pre-translated information, and additional information. Pre-translated information currently consists of that which has been drawn up in the tables specifying different offences in the criminal codes of the Member States. Transmitting information from, say, English to German authorities with the code 2301 00 would allow the interconnecting software to translate "unauthorised entry or residence" into German, using translations already supplied. Such a tool is likely to aid mutual understanding and the speed with which information can be exchanged.

However, potential problems with automatic translation are envisaged in the legislation. Paragraph 14 of the Preamble of *Council Decision 2009/316/JHA* states that:

"The accuracy of the codes mentioned cannot be fully guaranteed by the Member State supplying the information and it should not preclude the competent authorities in the receiving Member State from interpreting the information."[37]

It is for this reason that additional information may be necessary, in order to provide the receiving authorities with a better idea of the constitutive elements of a particular offence, or the specific nature of a sentence handed down. Yet this is apparently not obligatory, as is clear from Recital 13 of the Preamble:

*"In order to ensure the mutual understanding and transparency of the common categorisation, each Member State should submit the list of national offences and penalties and measures falling in each category referred to in the respective table. Member States **may** provide a description of offences and penalties and measures and, given the usefulness of such description, they should be encouraged to do so. Such*

35. *Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (the ECRIS), in application of Article 11 of Framework Decision 2009/315/JHA*, p.3

36. The full table is available in Annex A of *Council Decision 2009/316/JHA*.

37. *Council Decision 2009/316/JHA*, Recital 14

information should be made accessible to Member States."[38] (emphasis added)

The European Parliament attempted to amend this so that Member States would be legally obliged to "include a short description of the constitutive elements of the offence." [39] This was rejected by the Commission on the grounds that:

> *"The proposed obligation would be excessively burdensome for Member States and could lead to a considerable delay in the commencement of operation of the ECRIS. Some [Member States'] delegations have already expressed serious concern in this respect."*[40]

Similar problems arise with Article 5 of the *2009/316/JHA*, which states that "the list of national offences… may also include a short description of the constituent elements of the offence." A recommendation from the European Data Protection Supervisor that this be altered to make short descriptions obligatory was ignored.

Making the provision of information on the constitutive elements of each offence mandatory and ensuring a clear circumscription on the use of automatic translation may have been slightly more cumbersome for the authorities, but would have greatly increased the accuracy of the system. As it is, the legislation leaves ample room for misunderstandings between authorities in the transmission and receipt of information.

There are further issues regarding the identification of individuals. The European Union has numerous official alphabets. Translating individuals' names from one to another may well be a cause of problems, unless clear guidelines are put in place to ensure consistent methods of translation of names as well as offences. The differences between Latin, Greek and Cyrillic alphabets are obvious, and characters from the Polish, Lithuanian and other alphabets may also prove troublesome.

A further problem may be that of "multiple persons found." [41] In such a situation, when one state makes a request to another for information on an individual, or transmits information regarding a conviction, the information held by the requested state may not be extensive enough to attach the information to a single individual. The solution currently proposed to such a problem is that "the requested member state informs the requesting member state that the request cannot be answered." [42] The request would then have to be sent again with more detailed information.

---

38. EDPS, *Opinion*, 16 September 2008, para. 13

39. European Parliament, *Legislative resolution on the proposal for a Council decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA*, 9 October 2008, Amendment 2

40. Commission Position, *Legislative resolution on the proposal for a Council decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA*, p.1

41. The Polish Delegation, *Proposals of Poland regarding the chapter 5.2 of Business Analysis* 7401/11, 8 February 2011, p.2

42. Ibid., p.3

However, the receiving member state will be able to choose whether or not to retain the incomplete or incorrect information from a request that leads to "multiple persons found." This not only makes it more likely that sensitive information about an individual will be left unnecessarily in the database of a Member State other than that of the individual's nationality, but may also increase the likelihood of information being attached to the wrong person. While the ECRIS legislation permits Member States to attach fingerprints to criminal records for the purposes of identification, [43] only three Member States (Lithuania, Romania and the UK) have so far noted an interest in doing so. Furthermore, there is currently no certainty on how such exchange would take place via the system, and it therefore seems uncertain as to whether fingerprint exchange will begin at the same time as the general use of the system in April 2012. [44]

It is easy to envisage situations where mistranslated information could be used in court with negative repercussions for the individual(s) facing sentencing, while a failure to provide additional information on a particular offence or conviction may have similarly injurious effects. Furthermore, the potential for situations of "multiple persons found" may also lead to the wrong person(s) being subjected to criminal and judicial procedures until they are able to clear their name. Despite the legislation stating that the ECRIS "respects fundamental rights and observes the principles recognised in particular by Article 6 [right to a fair trial] of the Treaty on European Union and... The Charter of Fundamental Rights," [45] it is hard to see how this is the case when the system has such broad scope for error with regard to the accuracy of the information being transmitted.

'Common communication infrastructure'

The "common communication infrastructure" is the other technical aspect of the ECRIS. There will be no central database operated at the EU level. Rather, "criminal records data will be stored solely in databases operated by Member States," [46] which will be connected by the EU's S-TESTA (Secured Trans European Services for Telematics between Administrations) network. If the judicial (or other) authorities in one member state wish to access information on the conviction(s) an individual who is a citizen of another member state, they will have to submit a request to their own state's central authority, which will then make the request to the central authority in the state of nationality of the individual in question. The authorities in the state of nationality will then either provide all or some of the requested information, or refuse the request. Direct access by the authorities of one member state to the database of another member state will not be possible, and each member state will be responsible for the records in its own database and ensuring that the information contained in its criminal records is accurate and up-to-date. Any convictions received by an individual in a member state not that of his or her nationality are to be

---

43. *Council Decision 2009/315/JHA*, Article 11(c)(ii)

44. iLICONN, *ECRIS Technical Specifications – Inception Report*, 15458/10, 17 November 2010, p.81

45. *Council Decision 2009/316/JHA*, Recital 20

46. European Commission, *Electronic interconnection of criminal records- establishment of the European Criminal Records Information System*, 30 May 2010

transmitted to the individual's state of nationality as soon as possible, so that the criminal record can be updated.

As an example, an English national convicted of a crime in Italy would have the information regarding the conviction entered into a criminal record in Italy. It would also be sent back to England, where it would be entered into the individual's criminal record. If at a later date they were facing prosecution in Hungary, the Hungarian judicial authorities (knowing that they were dealing with an English national) would be able to request the individual's criminal record from England, which would contain the information regarding their conviction in Italy.

The basis for the ECRIS is the Network of Judicial Registers, a pilot project that has been running since 2003. Statistics from the project demonstrate that the minimum time for a reply to request was "a few minutes," with the average being "circa three hours." [47] Regardless of this speed, it would be surprising if in the future demands are not made for changes to the system, in order to improve technical aspects of its functioning. Such demands could potentially come in three forms.

Firstly, a proposal that all the relevant information should be centralised, allowing for greater ease of collection and access. Considering that this has been proposed in the past by the Council, such an idea may well surface again. Secondly, it is possible to envisage what may be termed access creep. Demands may be made that the idea of central authorities and competent authorities be altered or extended, allowing a greater number of access points to the network, for a greater number of people. It is already intended that the ECRIS will be used to exchange information not just for use in criminal proceedings, but also for employment and firearms licensing purposes. The expansion of access point is therefore certainly a possibility: an increasing number of authorities wanting to use the network would necessitate an expansion of access points so that the system could cope and users were satisfied. A third possibility is the demand that direct, cross-border access to other Member States' databases is made possible. As noted above, the forthcoming proposal for the ECRIS-TCN may well demand the establishment of a centralised database for convicted third country nationals. Finally, there is the potential for interoperability between criminal records systems and other databases. All of these potential developments may have unsavoury implications for civil liberties and fundamental rights.

Data protection and access to information

As noted, the ECRIS is based on two separate but related pieces of legislation, *Council Framework Decision 2009/315/JHA* and *Council Decision 2009/316/JHA*. The many shortcomings in both pieces of legislation, as well as the separate data protection framework by which they are governed (stemming from *Council Framework Decision 2008/977/JHA*) will be outlined here.

47. *Network of Judicial Registers*, 4 September 2007

Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from criminal records

It is clear from the opening recitals of this piece of legislation that data protection concerns were not paramount in the minds of its drafters. The European Parliament proposed that a new recital be added that made clear the Member State of nationality would be considered as the "owner" of information related to an individual, thus clarifying the responsibility of that State's authorities for ensuring that the data is accurate and up-to-date. In the main text, Article 5(2) states that any deletion of or alteration to information "shall entail identical alteration or deletion by the Member State of the person's nationality… for the purpose of retransmission in accordance with Article 7." The Parliament proposed that the phrase "for the purpose of retransmission in accordance with Article 7" be deleted. [48] It also proposed that the same phrase be deleted from Article 5(3). Although no justification was provided for the amendment, it is reasonable to assume that it was intended to clarify that only accurate and up-to-date information may be used for any purpose, rather than just retransmission. However, neither amendment was included in the final text.

Article 6 of the legislation concerns requests for information on convictions. These will come from the central authority of another Member State, but may have been made to that authority by law enforcement authorities, employers, licensers, or other bodies. There is no obligation on the central authorities of the Member State to pass on that request to the other Member State (they "may, in accordance with… national law"). However, if they do choose to make such a request, they are under no obligation to state for what purposes that request has been made, other than that it is from a judicial or competent administrative authority, or from the individual concerned. Article 7 states that the requested Member State "shall reply in accordance with its national law." The EDPS recommended that requests for purposes other than criminal proceedings should only be allowed "under exceptional circumstances." [49] The proposal for such a stringent limitation was ignored. Depending on the national law in different Member States, the legislation provides an opportunity for the widespread cross-border exchange of information extracted from criminal records for a variety of purposes unrelated to criminal proceedings.

Article 9 of *2009/315/JHA* deals with conditions for the use of personal data. The European Parliament proposed that two entirely new paragraphs be added to the article, in order to specify and strengthen the data protection obligations on the authorities in the Member States. [50] While the proposed articles merely pointed out basic principles of data protection – that processing shall be lawful, necessary and proportionate; collection of data will be for specific and limited purposes; that data shall be accurate and up-to-date; and that sensitive information such as ethnic origin or political opinion would be processed only under specific safeguards – they were rejected.

---

48. European Parliament, *Legislative resolution*, 9 October 2008, Amendments 6 and 7

49. EDPS, *Opinion*, 29 May 2006, para. 57

50. European Parliament, *Legislative resolution*, 17 June 2008, Amendments 10 and 11

Article 9(3) permits the use of information "for preventing an immediate and serious threat to public security." Further safeguards were rejected that would have provided limiting conditions. These suggested that the use of information under 9(3) should be permitted if it were "necessary and proportionate," and that if this happened, a justification would have to be provided that outlined how the conditions of "necessity, proportionality, urgency and seriousness of the threat" were fulfilled. No such limitations or safeguards were included in the final text.

Although Member States' central authorities will be subject to national data protection legislation, the provisions of Article 9 make no reference to data protection authorities, something noted by the EDPS. [51] Given that the ECRIS is intended to play a part in the creation of a common culture amongst law enforcement bodies in Europe, it may have been beneficial to include a provision requiring national data protection authorities to work together, "so as to enable an effective supervision on aspects of data protection, in particular on the quality of data." [52] As with so many of the other recommendations and amendments that would have placed more stringent safeguards on information exchange, and ensured more effective oversight, the suggestions regarding data protection authorities were also ignored.

Finally, it should be noted that an attempt made by the European Parliament to simplify the procedure through which individuals can access information contained in their criminal record was rejected by the Commission and the Council. Article 6(2) of *Council Decision 2009/315/JHA* outlines the obligations of states with regard to requests from individuals for information on their own criminal records. The legislation reads as follows:

> *"When a person asks for information on his own criminal record, the central authority of the Member State in which the request is made may, in accordance with its national law, submit a request to the central authority of another Member State for information and related data to be extracted from the criminal record, provided the person concerned is or was a resident or a national of the requesting or requested Member State.*" [53]

The amendment would have replaced the word "may" with "shall", providing an obligation for the requested Member State to request from all other relevant Member States the information held on the individual's convictions. The European Data Protection Supervisor made a similar recommendation in an *Opinion on the Proposal for a Council Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States*. [54]

---

51. European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States (COM (2005) 690 final)*, 29 May 2006, para. 49

52. Ibid., para. 49

53. *Council Decision 2009/315/JHA*, Article 6(2)

54. EDPS, *Opinion*, 29 May 2006, p.10

The limitations of the legislation will make it the process of seeking recourse for inaccurate, incorrect or false information with national data protection authorities lengthier and more complex. Seeking adjustments, amendments or correction will be possible (although not necessarily easy) in an individuals' home state or state of nationality, but doing so in other Member States may be more difficult. An amendment tabled by the European Parliament that would have obliged the authorities of the state in which the request was made to transmit that request to the central authorities of other Member States was rejected.

Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA

As with *2009/315/JHA*, numerous recommendations and amendments that would have improved its data protection provisions were suggested for *2009/316/JHA*. Those which were incorporated into the final text were of little real significance.

Article 3 outlines what the European Criminal Records Information System is, and how it is intended to work. Article 3(3) states that:

> *"The best available techniques identified together by Member States with the support of the Commission shall be employed to ensure the confidentiality and integrity of criminal records information transmitted to other Member States. "*

However, no mention is made of data protection authorities, who would presumably be well-placed to advise Member States on how to ensure confidentiality and integrity. As it is, there is no statutory provision requiring the involvement of national or European data protection authorities.

Perhaps the biggest problem is to be found in Article 3(6), which notes that the "common communication infrastructure shall be operated under the responsibility of the Commission." This fact implies that the Commission "must be seen as the provider of the network." [55] It follows from this that the Commission is responsible as a data controller when:

> *"Personal data are processed in connection with the provision of the network or if data protection issues arise in connection with the security of the network."* [56]

However, because of the fact this was third pillar legislation:

> *"Regulation (EC) No 45/2001 [on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data] does not automatically apply, nor does any other legal framework on data protection and on supervision apply to the processing activities of the Commission."* [57]

---

55. Ibid., para. 23

56. Ibid.

57. Ibid.

It was therefore proposed by the EDPS that a specific provision be added, to ensure that processing undertaken by the Commission would be governed by Regulation (EC) No 45/2001. The failure to include such a provision provides another example of the European Union's more powerful bodies ignoring an opportunity to provide a higher level of data protection.

The responsibility for ensuring that Member States' software systems work with one another has also been left to the Member States themselves. While the Commission has responsibility for ensuring that logging and statistics-gathering is undertaken effectively, it has no role in ensuring the overall conformity of Member States' software. With no oversight at the European level, solutions to any problems that may arise with the software will be harder to coordinate. The Parliament made a recommendation that the Commission be given explicit responsibility for this by adding a new provision to Article 3(7), [58] but it was not included in the final text.

Recommendations for Article 6 (which addresses implementing measures, such as the drawing up of a manual for practitioners and establishing systems for the collection of statistics) were also ignored. The EDPS suggested that "in Article 6 reference must be made to a high level of data protection as a precondition for all the implementing measures to be adopted." [59] The failure to include such a reference is another indication of the attitude of the Commission and the Council to data protection principles. Furthermore, Article 6(1) states:

> *"The Council, acting by as qualified majority and after consulting the European Parliament, shall adopt any modifications of Annexes A and B [the tables of offences and penalties] as may be necessary."*

Questions may of course be raised regarding what the Council considers necessary. There are also serious concerns over the nature of Council consultations with the Parliament – that is to say, such consultations are frequently little more than an exercise in public relations, and can readily be ignored. [60] It is likely to be some time, however, before any amendments to the legislation are officially proposed, considering that the system itself is not yet functioning.

Finally, Article 7 obliges the Commission to publish regular reports detailing the exchange of information via the ECRIS. These reports are to be based "in particular on the statistics referred to in Article 6(2)(b)(i)". This article is rather vague, merely stating that reports should include "non-personal statistics relating to the exchange through ECRIS of information extracted from criminal records." It is vital that any evaluative reports do not

---

58. European Parliament, *Legislative resolution*,9 October 2008, Amendment 6

59. European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment of the European Criminal Records Information System (the ECRIS) in application of Article 11 of Framework Decision 2008/…/JHA*, 16 September 2008, para.42

60. For an examination, see Statewatch's *Guide to decision-making and justice and home affairs after the Treaty of Lisbon*: in particular the section covering non-legislative acts based on secondary legislation

merely focus on the technical aspects of the system by, for example, providing details on the number of exchanges made between which Member States.

A recommendation was made by the EDPS that the statistical data collected by the Commission should include that related to individual requests on personal data, the number of corrections made to personal data, the "length and completeness of the update process, the quality of persons having access to these data as well as the cases of security breaches." [61] These factors are not included in the text, but their inclusion would have helped make clearer not just whether information is being exchanged, but also what quality of information is being exchanged and whether the system is functioning to a standard that provides a high level of protection for data and other fundamental rights.

It should be clear that in the drafting of the two pieces of legislation that form the basis of the ECRIS, the majority of recommendations that would have strengthened the rights of data subjects and improved the quality of data exchanged through the system were rejected or ignored. It seems that the concern of the Commission and the Council lies not with these principles but rather with easing the work of Member States' law enforcement authorities. The next piece of legislation under consideration provides a clear display of these concerns.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

This infamous document is the primary piece of legislation governing the protection of data exchanged through the ECRIS. It has been remarked of the drafting process that "the Council... simply ignored all the criticisms... from the European Parliament, the European Data Protection Supervisor, the Article 29 Working Party on Data Protection, and civil society." [62] This is perhaps why: "almost each and every [principle] comes with an exemption that opens the door to the police to do otherwise than the principle prescribes, if they see fit." [63] An October 2006 speech by Lord Avebury took umbrage with the involvement in drafting legislation of working groups such as the Multidisciplinary Group on Organised Crime, pointing out that this group's primary purpose was:

> *"to make life difficult for criminals, not to have regard to the interests of data subjects."*[64]

Furthermore, he noted that the problem with such groups is that:

---

61 Ibid., para.36

62. Statewatch Observatory on data protection in the EU

63. Paul de Hert and Vagelis Papakonstantinou, 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for' in *Computer Law & Security Review*, 25 (2009), p.411 (subscription required)

64. Lord Avebury, speech given at the European Parliament to the Joint Parliamentary Meeting on EU developments in the area of freedom, security and justice, 3 October 2006, p.3

> *"[T]hey seek to pre-empt EU decision-making processes, by making arrangements of their own, and offering them to other Member states on a take-it-or-leave-it basis."*[65]

Although the legislation was opposed by a wide number of groups and individuals and was delayed for over a year, it was eventually passed. The general tone can perhaps be best summed up by the following excerpt, from Recital 11 of the Preamble:

> *"It is necessary to specify the objectives of data protection within the framework of police and judicial activities and to lay down rules concerning the lawfulness of processing of personal data in order to ensure that any information that might be exchanged has been processed lawfully and in accordance with the fundamental principles relating to data quality. At the same time* ***the legitimate activities of the police, customs, judicial and other competent authorities should not be jeopardised in any way****."*[66] (emphasis added)

Clearly, the activities of the "police, customs, judicial and other competent authorities" (whoever they may be) take precedence over the rights of individuals to privacy and data protection – rights which are not even mentioned in the above paragraph. It has been demonstrated that the prioritisation of the needs of law enforcement authorities was clear throughout the drafting process, [67] a fact amply demonstrated by the resulting legislation. In many ways the principle of "business-driven development" referred to in the Stockholm Programme provides an even stronger basis for working groups to have a significant level of influence over the legislative process, creating a formalisation of informality.

The disregard for supposedly fundamental rights and freedoms is borne out in a numerous other places in the document – for example, when data is transferred to third states or international bodies, the data transferred "*should, in principle*, benefit from an adequate level of protection" (emphasis added). [68] Presumably, principle can be overridden by political need.

Information exchange between EU Member States and third countries is also eased by the legislation. To quote de Hert and Papakonstantinou again: "under the [Data Protection Framework Decision] the web of international data transfer of EU criminal records is practically impossible to follow, even less to control." [69] This is due in part to the fact that the protection of data from processing other than for the purpose for which it was collected, covered by Article 3(1), is rendered void by Article 3(2), which states that:

---

65. Ibid., p.2

66. *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,* Recital 11

67. Statewatch Analysis, *EU data protection in police and judicial cooperation: Rights of suspects and defendants under attack by law enforcement demands*, October 2006

68. *Council Framework Decision 2008/977/JHA,* Recital 23

69. de Hert and Papakonstantinou, 'The data protection framework decision of 27 November 2008', p.412 (subscription required)

"Further processing for another purpose shall be permitted in so far as:

(a) it is not incompatible with the purposes for which the data were collected;
(b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions;
(c) processing is necessary and proportionate to that other purpose.

The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous."

This article in fact makes a mockery of the purpose specification principle:

"Given that the whole DPFD is about police and judicial processing, the purpose specification principle may in practice always be bypassed, because personal data shall always be collected for police processing purposes and processing under the DPFD shall thus never be 'incompatible with the purposes for which the data were collected."[70]

The provisions governing the use of data transmitted through the ECRIS therefore do not provide sufficient protection for there not to be a risk of the authorities going on to do as they wish with the data that has been received. As has been noted, use of the system has already moved beyond the realm of judicial proceedings and into employment and firearms licence vetting. *Council Decision 2009/315/JHA on the organisation and content of information extracted from criminal records* allows Member States to request criminal record information for purposes other than criminal proceedings, to which the requested member state must "reply in accordance with its national law." [71] Although it is of course not obligatory for the requested Member State to reply, the door is open to requests from any individual or institution that can demonstrate a 'legitimate' interest in an individual's criminal records. Combined with the weak protections of *2008/977/JHA,* the possibility of information shopping arises. Law enforcement (or other competent authorities) may not be able to obtain information on an individual from that person's home state, but it may be accessible via a state which also holds the information and has less stringent data protection legislation.

Following the entry into force of the Lisbon Treaty and the dismantling of the pillar structure, the European Commission is faced with the task of revising current data protection instruments and developing a comprehensive framework for data protection in the EU. Data protection in police and judicial co-operation will be covered by this. However, it remains to be seen whether the new legislation will resolve the flaws in the current regime, while the process by which legislation is drafted is still in need of fundamental reform. The loopholes and discrepancies in both the legislation establishing the ECRIS, as well as the data protection regime governing the system, provide too much scope for the misuse of individuals' personal data.

---

70. Ibid., p.411

71. *Council Decision 2009/316/JHA*, Art. 6(1) & Art. 7(2)

Domestic problems

Aside from the issues of proportionality and privacy raised by such a project, the ECRIS is also likely to exacerbate existing problems within the criminal justice systems of Member States. The *ECRIS Technical Specifications - Inception Report* states that:

> *"It is assumed that the information on criminal records transmitted by each Member State's central authority to foreign Member States' central authorities is always* ***correct and complete****."*[72] (emphasis in original)

This may be over-optimistic. The British press has in recent years reported a number of issues regarding both the accuracy of criminal records and the maintenance of criminal records databases. In August 2009, it was reported that "hundreds of innocent people have been accused of wrongdoing by the CRB [Criminal Records Bureau]." In the twelve months between April 1st 2008 and March 31st 2009, 1,570 people checked by the CRB were "wrongly given criminal records, mistakenly given a clean record or accused of more serious offences than they had actually committed." [73]

More recently, press reporting of the *PNC* [Police National Computer] *Inspections: National Overview* report focused on the fact that there was information on over 35,000 court cases waiting to be entered upon the Scottish database. This was blamed on "a lack of direction at senior level," and the fact that the "flow of information" between the three main criminal justice agencies (the police, prosecution service and courts) "needs to be more robust... to prevent omissions and failures." [74] Any problems that exist with transferring information from one authority to another *within* a state cannot be resolved by the ECRIS, an instrument designed to facilitate the transfer of information *between* states. Indeed, by increasing the exchange of criminal records between states, the ECRIS will almost certainly exacerbate problems with inaccuracies, firstly by making them subject to mutual recognition and thus validating them, and secondly by spreading them across two or more Member States and thus making rectification more difficult for the individual concerned. Other EU Member States may suffer from problems similar to those in Britain. With this in mind, the chances of an individual having inaccurate or incorrect information from their own criminal record held against them in court increase.

There is also the fact that any request made by an individual to have data about themselves rectified will now have to travel through the authorities in their own state, as well as any other state which may be holding information on them. This multiplies the chances of rectification being done badly or not at all. It also raises the possibility of incomplete correction - for example, data may be rectified in some Member States but not others. The EDPS has remarked of this problem that "[a]dditional measures are needed, for instance to ensure that the information kept by the sending and receiving Member State (state of

---

72. Council of the European Union, *ECRIS Technical Specifications – Inception Report*, 15458/10, 17 November 2010, p.68

73. Christopher Hope, 'Criminal Records Bureau errors lead to hundreds being branded criminals', *The Daily Telegraph*, 2 August 2009

74. *Scottish criminal record accuracy questioned*, BBC News, 04 August 2008

conviction and state of nationality) are kept up to date and identical." [75] What these "additional measures" could be is not mentioned. Regardless, no such measures are available in the legislation. It is potential situations such as this that may lead to demands for the centralisation of criminal record databases, in the name of enhancing accuracy and lessening the workload of those responsible for updating records.

Conclusions

Something as sensitive as an individual's criminal record should be subject to the most stringent protections available when it comes to translating, transmitting, and using the information contained within. Ongoing discussion about the implementation of the ECRIS will be undertaken by the Working Party on Cooperation in Criminal Matters, [76] with the "possibility" of meetings with the Commission's Expert Group on Criminal Records. As such, there is no room for any long-term, meaningful consultation with representatives of data protection authorities, although the significant lack of data protection provisions in the legislation is perhaps indicative of the fact the involvement of such authorities is not particularly welcome in projects intended to increase the punitive and coercive powers of state authorities. The recommendations and amendments suggested by the European Parliament, the European Data Protection Supervisor, and civil society group were all largely ignored, [77] to the detriment of protections for individuals.

The legislation establishing the ECRIS, the ideas on which it rests, and its disproportionate application to all criminal records (and subsequent extension to vetting and supervision measures) are all significantly problematic. It is highly questionable whether information on all offences should be exchanged and as such the possibility of excluding convictions for minor crimes from the system should be a matter of debate. Furthermore, the ongoing development of the practitioners' manual, in which the definition of conviction has been extended to include non-criminal rulings, should be subject to wider scrutiny. At some point use of the ECRIS will infringe one or more of the rights listed in the Charter of Fundamental Rights of the European Union, which the system supposedly respects. The system as a whole is constructed in such a way as to allow ample scope for the abuse and misuse of information contained in criminal records.

4. The European Police Records Index System (the EPRIS)

Basic principles

The EPRIS is intended to be:

> *"A system which gives Member States' law enforcement authorities a quick overview of*

75. EDPS, *Opinion*, 19 September 2008, Art. 19

76. Presidency, *Exchange of information extracted from criminal records (the ECRIS)*, 6396/10, 24 February 2010, p.2

77. Association européenne pour la défense des droits de l'homme, *The European Criminal Records Information System (ECRIS) creates new risks for the protection of personal data*, 23 October 2008; Fair Trials International, *Statement on the European Criminal Records Information System (ECRIS)*, 30 June 2008

> *whether and possibly where relevant police information on a certain person can be found. It was stated that this would facilitate requesting detailed information and complement Council Framework Decision 2006/960/JHA [the Swedish Framework Decision] in particular, making it easier to detect cross-border connections and identify structures of international organized crime or terrorist networks. Secondly, the information gained in this way would significantly help in protecting the police officers assigned to the case."*[78]

It is thus an attempt to simplify the exchange of information and intelligence amongst police forces, with the proposal currently limited to international organised crime and terrorism.

From the above description it seems that the EPRIS is intended to be an index rather than a medium for the actual exchange of information, using a 'hit/no hit' system to tell the user whether the desired information exists. While a search may reveal that a particular police force holds a record related to a person, the record would have to be obtained through a request to the police force that held the information. The principle of availability would of course apply to any such requests, with the provisions of the Swedish Framework Decision necessitating a swift reply.

Origins and development of the system

The idea for the EPRIS stems from the German government, whose delegation to the Police Chiefs Meeting in April 2007 presented a proposal for a system designed to provide an index of "police criminal records". [79] Later meetings demonstrate that the enthusiasm of some states for such a system was tempered by others, who:

> *"Urged for more caution and pointed to the need for a feasibility study regarding this proposal, which would consider the legal, technical and financial aspects, as well as the impact at national level."*[80]

It was not until November 2009 that agreement on such a "pre-study" could be reached. The German delegation entered a reservation on the decision made to conduct a pre-study, stating that "business needs and added value are already established and the study should deal with solutions." [81]

Despite having had to wait slightly longer than they wanted, the German government had its wish for solutions granted when the Commission's pre-study "confirmed the need for action." [82] The process of finding a private contractor to complete the next stage of development has now begun. The tender released to attract private contractors states that:

---

78. Presidency, *European Police Records Index System – elements for a pre-study*, 15526/2/09, 21 December 2009, p.1

79. Police Chiefs meeting, *Outcome of proceedings*, 8324/07, 23 April 2007, p.2

80. Police Chiefs meeting, *Summary of discussions*, 16191/07), 11 December 2007, p.2

81. *European Police Records Index System – elements for a pre-study*, p.1

82. Ad hoc Group on Information Exchange, *Summary of Discussions*, 11536/10, 2 July 2010, p.6

> *"The general objective of this study is to present a complete and structured overview of the definitions of a "police record" existing in all EU Member States and in the Union acquis as well as formulating proposals for a definition of the term "police record" at the EU level and of possible ways in which efficiency in exchange of police records between the Member States could be enhanced by setting up an IT index system related to police records."*[83]

The successful contractor will be provided with a significant amount of scope with regard to what it may propose for the system. They are obliged to provide at least four definitions of the term "police record" at EU level, as well at least four "different options for possible IT architecture solutions for a hit/no-hit system and an index system." There is nothing in the proposal to indicate that a proposal for direct access to Member States' databases would be rejected, although such a suggestion would certainly cause significant political friction.

Allowing a private contractor to define what constitutes a police record brings a different meaning to the idea of business-driven development put forth in the Stockholm Programme. Allowing both law enforcement authorities and businesses to drive the development of systems for information exchange may well contribute to permissive approaches to the exchange of information, and expansive approaches to definitions of terms such as police record.

Member States have raised concerns over the project. At a meeting in July 2010, "on doubts of several delegations as to the need for such an IT solution, the Commission referred to the mandate in the Stockholm Programme." [84] More recently, Sweden has criticised the Commission's lack of transparency in the development of the system, demanding that answers to questionnaires on which the need for a system was based be shared amongst all Member States before they are disclosed to bidders for the contract. Furthermore, the Swedish delegate "questioned the conclusions drawn by the Commission since the sample was rather limited and the need for EPRIS could have been interpreted in a quite opposite way." That is, the system may not be necessary at all. Yet there seems to be a strong interest at the Commission in developing the EPRIS. Other delegations were "critical about details of the study concept since they were afraid that a police data base might be set up instead of [a] record index." In response, the Commission "denied that an EU police database was envisaged and pledged to involve Member States in the development of the project." This will involve ensuring the Working Party on Information Exchange and Data Protection is kept informed of developments. How much input they will have into the project – and whether such input would even be beneficial to the rights of individuals - remains to be seen.

Proportionality and scope

As with the ECRIS, there are serious questions of proportionality. Although the paragraph describing the EPRIS quoted above provides justifications of terrorism and international organised crime, there is no indication that the system will be limited only to the police records of those suspected of involvement in such activity. The application of the principles

---

83. European Commission, *Call for tender no. HOME/2010/ISEC/PR/068-A3*, 8 April 2011, p.9

84. Ad Hoc Group on Information Exchange, *Summary of discussions*, 11536/10, 2 July 2010, p.6

of availability to matters involving the exchange of information between police and judicial authorities mean that any such limitations may effectively become null and void. Indeed, it is likely that those responsible for the development and implementation of the EPRIS are thinking in far broader terms.

The prevention of some individuals from entering Denmark before the COP15 summit in Copenhagen in December 2009; the pre-emptive arrest of hundreds of protesters in both Copenhagen [85] and more recently in Brussels; [86] and the scandals surrounding the transnational use of police infiltrators in protest groups [87] demonstrate that police forces in Europe are prepared to co-operate to prevent individuals exercising the right to protest, an activity that has nothing to do with terrorism or international organised crime. In the context of this kind of police work, undertaken with the approval of the governments to which the police are responsible, it is clear that the EPRIS will work to boost "the transnational enforcement capacity of governmental actors," [88] and increase the power of the state in relation to the individual, even when those individuals are attempting to exercise a fundamental right.

Further potential problems stem from the fact that police records can contain either hard information – verifiable facts – or soft "intelligence", which can be based on suspicion, informants, rumour etc. Grading systems are used by police forces to evaluate the reliability of information and intelligence. When a particularly low grade is assigned to this data it may suggest that "the intelligence is unreliable and [its] exchange should be prohibited." [89] The table on the following page provides the standard ways in which EU law enforcement authorities interpret data they receive. Subjecting inaccurate "intelligence" to the process of mutual recognition may well see it recognised as valid information in another Member State. The EPRIS may provide a significant possibility for low-grade information to be disseminated throughout European police forces, all of whom have differing cultures and standards. Any such dissemination may have injurious effects upon individuals.

Similar problems are also liable to arise with the ECRIS, where a judgement made by a court in one member state, even if it is, for example, based on false evidence or bribery, comes to be validated through the process of mutual recognition. This is demonstrative of a wider problem with attempts to increase police and judicial co-operation through mutual recognition: while it serves the purpose of increasing co-operation without harmonisation, it also exports any flaws that exist within the criminal justice systems of the Member States of the European Union.

---

85. Bibi van der Zee, 'Protests in Copenhagen: Rights groups press for inquiry into police tactics', *The Guardian*, 13 December 2009

86. No Border Bxl, *Call Out Against Repression*, 12 January 2011

87. Euro-Police, *Cross-border spying on "Euro-anarchists"*, 23 February 2011; see also the extensive coverage that *The Guardian* has provided on the cases of Mark Kennedy and other police spies.

88. Lavenex, 'Mutual recognition and the monopoly of force', p.765

89. Statewatch Analysis, *Rights of suspects and defendants under attack*, p.6

Europol handling codes [90]			
The source of the information shall be indicated as far as possible on the basis of the following criteria:		**The reliability of the information shall be indicated as far as possible on the basis of the following criteria:**	
A	Where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances	1	Information whose accuracy is not in doubt
B	Source from whom information received has in most instances proved to be reliable	2	Information known personally to the source but not known personally to the official passing it on
C	Source from whom information received has in most instances proved to be unreliable	3	Information not known personally to the source but corroborated by other information already recorded
D	The reliability of the source cannot be assessed	4	Information which is not known personally to the source and cannot be corroborated

Concerns over the functioning of the judicial and police authorities in different EU Member States are not something that should be dismissed out of hand. While the European Union's Member States have all ratified the Council of Europe's European Convention on Human Rights (to which the EU itself is also due to accede), as well as being bound by the principles of the Charter of Fundamental Rights of the European Union, there are frequent and clear indications that not all Member States are able or willing to practice equal commitment to the principles of human rights and the rule of law. [91] While police and judicial cooperation driven by mutual recognition may lead to the raising of standards across Europe, there is also the danger of a "race to the bottom in the level of regulations." [92]

Data protection and conclusions

Until the drafting and passing into law of the EU's new data protection legislation, the EPRIS will be subject to the provisions of the *Framework Decision on the protection of personal data in the framework of police and judicial cooperation in criminal matters*, meaning that any information exchanged through the system would be subject to the same loopholes and get-out clauses as information exchanged through the ECRIS. Whilst a major issue in itself, the problems caused by this are exacerbated by the fact that the exchange of information facilitated by the EPRIS may well be entirely disproportionate to the stated aims of tackling terrorism and international organised crime. The Stockholm Programme declares that "the Union should aim for the systematic exchange of information." [93] The EPRIS is intended to assist in this systematic exchange, but before its development is agreed upon it must be

90. Statewatch News Online, *EU police intelligence handling codes*, August 2004

91. See, for example, the Statewatch Observatories on "Rendition"; Reactions to Protests; or the recent phone-hacking scandal that has plagued the Metropolitan Police in Britain.

92. Lavenex, 'Mutual recognition and the monopoly of force', p.765

93. *The Stockholm Programme*, p.23

submitted to wider scrutiny. Serious questions should be raised about the principles, proportionality and scope of the system.

5. Information Exchange Platform for Law Enforcement Authorities (the IXP)

The purpose and scope of the system

This project was initially entitled the Police Information Exchange Platform, [94] and was proposed by the Spanish Presidency of the EU in January 2010. The change in name reflects a change in purpose, shifting solely from "police information" to information required by "law enforcement authorities." The basic idea is to provide a central access point to every law enforcement information exchange tool that exists at EU level.

There is no mention of the project in the Stockholm Programme, but following its proposal by the Spanish Presidency in January 2010 the idea was then developed in tandem with Europol, who are currently leading the project. The current participants are Belgium, Germany, Spain, Lithuania, Hungary, Slovakia and the Commission. The project is very much in its infancy, although a report on how the system would be organised and how it would function is due to be published. [95] Nevertheless, the core ideas behind the system are clear. The "Business Concept" for the IXP outlines three "essential characteristics" of the project. [96] Firstly, it will be based around:

> *"A single website that serves as the starting point for any product or service related to international law enforcement cooperation [meaning] efficiency in development and maintenance, easier management of data protection, the enhancement of a shared experience as well as the user-friendliness of recognising and easily finding contacts and services in other Member States."*

Secondly, it will be made available to:

> *"The entire law enforcement community in the EU. This includes local, regional and national police forces, customs, coast guard and border control authorities. Also international law enforcement bodies, like FRONTEX [The European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union], OLAF [European Anti-Fraud Office], Interpol, EMCDDA [European Monitoring Centre for Drugs and Drug Addiction], CEPOL [European Police College], EuroJust and Europol should have access. It can also be extended to other institutions, such as* ***DG JLS [Directorate-General for Justice, Freedom and Security, now DG Home Affairs and DG Justice and Fundamental Rights], the Council Secretariat General,*** *but also judicial, prosecution and penitentiary services, where relevant. In principle, even non-EU partners could be given access, like the non-EU Schengen partners Norway, Iceland, Liechtenstein and Switzerland."* [emphasis added]

---

94. Council of the European Union, *Draft Action list for the implementation of the IMS*, 16951/1/09, 18 January 2010, p.19

95. Presidency, *Draft interim report on the Implementation of the 1st Action List*, 8420/11, 15 April 2011, p.3

96. Council of the European Union, *Business Concept for an Information Exchange Platform for Law Enforcement Agencies*, 1117/10, 15 June 2010, p.2

Finally, the IXP:

> Should provide any available answer to operational needs for cross-border law enforcement cooperation. To this end the IXP gives access (or re-directs) to relevant tools, channels, and information without affecting the applicable access management, security or data protection measures in place. It also assists the end-user in finding the appropriate products and services on the basis of the concrete needs for cross-border law enforcement cooperation.

Alongside the three "essential characteristics" are four different, wide-ranging categories into which tools available through the IXP will be organised. [97] The first of these is "knowledge management," which includes "documentation needed in general as background information or to understand how certain matters are organised," e.g. "legislation, forms, policy documents, tutorials, handbooks and guidelines"; national information pages for Member States and third countries, detailing "the law enforcement structure, data protection authorities, legislation, national peculiarities as well as contact points"; information on EU bodies, e.g. for authorities such as FRONTEX, OLAF, or Europol; and finally "dedicated environments" for "specific purposes" so that "law enforcement experts [can] communicate among each other."

Second is "tools". This will include EU law enforcement tools, which will be useful to "joint investigation teams, joint police and customs operations, common police teams and patrols, major events teams... EU law enforcement missions abroad etc."; shared tools "that were jointly developed or made available for common use [such as tools for] data mining, analysis or the monitoring of the internet and open sources consultation"; translation tools; and a live news publishing service.

The third category is "operational queries" which is intended to allow "a search capability that processes queries across the relevant databases managed in the framework of justice, liberty and security, and potentially also national databases." It is worth noting that the inclusion of "potentially" is somewhat moot, as the EPRIS would be accessible through the IXP and thus national databases will have to be included for searching. It is mentioned in a number of other places in the document that "[t]he processing must respect access restrictions established in the respective legal framework of the different databases, as well as any other applicable data protection conditions." Considering the scale and scope of such an operation, as well as the opportunities for rule-breaking that centralised access will facilitate, it is questionable whether safeguards stringent enough to maintain these principles can be introduced and upheld.

The fourth and final category is "communication channels," which makes note of the intention to link the IXP to Interpol's I24/7, Europol's messaging service SIENA (Secured Information Exchange Network Application), and the SIS communication system, SIRENE (Supplementary Information Request at the National Entry).

---

97. Ibid., p.2-3

Potential problems with the system

The idea that individual rights to privacy and data protection will be better safeguarded through the use of a single website in some ways makes sense, allowing as it does one route through which data protection authorities can monitor access and usage logs for each individual instrument. However, the technical hurdles that would need to be overcome in order for such a project to work – let alone to work securely - are vast. It is perhaps with such problems in mind that proposals have been tabled for an EU Police Information Model (EU-PIM), which would encourage a standardised format for all future information gathering and exchange tools developed by police forces in the European Union. [98] The application of differing national data protection regimes to the information potentially available via the IXP may also prove problematic.

There are of course problems beyond those of data protection and privacy. Most disturbing is the suggestion that access should be extended beyond law enforcement agencies, employed to enforce the law, to the EU Directorate-Generals of Home Affairs and Justice, as well as the Council's General Secretariat. These bodies should have no role in accessing personal data or operational information that may be available through a system such as the IXP. They should not have any access at all. Such a proposal is extremely dangerous in its implications for the democratic principle of the separation of powers between the institutions of government and the law. It is, however, demonstrative of the thinking prevalent within some policy-making circles: the greater the level of information-sharing, the better.

As with the ECRIS and the EPRIS, it seems that there would be a serious likelihood of access creep as authorities able to use some tools available through the IXP make demands for access to others. There is also the possibility that the already-extensive list of bodies that should be given access to the platform will be extended even further, as has happened with the granting of access to the ECRIS for those responsible for vetting employment and firearms licensing. The "entire law enforcement community" is not a static entity, and the inclusion of new bodies in such a community is a clear possibility, as has been amply demonstrated with the development of the Schengen Information System, to which even institutions such as the Polish military now have access. [99]

Furthermore, providing access to all information "products" (as the documentation refers to them) through a single point of entry leaves the system wide open to abuse in situations where an individual whose access is restricted to particular tools shares workspace, or has a working relationship, with another individual who is able to access more information than them. EU authorities were themselves surprised when the number of terminals able to access the Schengen Information System grew from 55,000 in 1999 to 'approximately

98. German Delegation, *IMS Action List – European Police Information Model (EU-PIM)*, 5486/10, 19 January 2010, p.2

99. General Secretariat of the Council, *List of competent authorities which are authorised to search directly the data contained in the Schengen Information System pursuant to Article 101(4) of the Schengen Convention*, 9455/1/11, 17 May 2011

125,000!!!' in March 2003. [100] The number of access points now stands at more than 500,000, a nearly ten-fold increase in just over ten years. [101] It remains to be seen how the creation of another EU-wide information exchange tool will increase accountability and improve the protection data subjects' rights, as proposals for the IXP have claimed. Indeed, it is questionable whether such a system is justifiable.

6. Conclusions

The principles of availability and mutual recognition, in tandem with the ideal of creating a "common law enforcement culture", are permitting the profusion of a vast number of different systems designed to facilitate the exchange of information between different law enforcement bodies. While there are undoubtedly valid reasons for exchanging limited amounts of information from individuals' criminal and police records within the EU, attempts to make the exchange of information on criminal records and police records simple and systematic will seriously infringe a number of supposedly fundamental rights. The way in which the legislation surrounding the ECRIS is drafted shows little concern for this fact, with the legislation's own data protection provisions weak, and the wider data protection framework that covers the system largely a tool for police and judicial authorities to do as they wish with individuals' data. The Commission is also devoid of any responsibility for information exchanged through a system for which it can be regarded as a controller. These shortcomings are the result of a desire to permit the swift and systematic exchange of information extracted from criminal records, combined with a political system that enables the Commission and the Council to effectively ignore the recommendations of those bodies who have to be relied upon far too often to stand up for the rights of individuals.

The Commission is due to publish its first report on the application *Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from criminal records* in April 2015, which will be accompanied "if necessary by legislative proposals." This may provide an opportunity to demand the implementation of more stringent data protection safeguards or even limitations on the types of information to be exchanged. Of course, it may also provide an opportunity to permit the exchange of an even wider variety of information than that which is already planned. Meanwhile, a report on the application of *Decision 2009/316/JHA*, due in 2016, [102] is likely to be a statistical report based on records of the exchange of information. It remains to be seen whether either of these reports will take into consideration any miscarriages of justice or misuses of personal data that may have taken place.

Both the EPRIS and the IXP are still largely in the planning stage. Nevertheless, a considerable amount of time, energy and resources have already been invested in both systems. The bureaucratic inertia created by this and the political support that already exists for the projects will make it harder for those opposed to the system to make their voice

100. Statewatch Analysis, *From the Schengen Information System to SIS II and the Visa Information System (VIS): the proposals explained*, p.7

101. Jamie Doward, '500,000 EU computers can access private British data', *The Guardian*, 7 February 2010

102. Council Decision 2009/316/JHA, Art. 7

heard, as some Member States' delegations have already found upon raising objections to the EPRIS. The secretive and frequently inaccessible workings of the EU's many working groups will also make wider scrutiny by parliamentarians and the public difficult. Systems such as the ECRIS, the EPRIS, and the IXP are merely symptoms of a wider problem – the use of mutual recognition and the principle of availability to increase cooperation between the police and judicial authorities of Member States, with no real questioning of whether such cooperation is desirable or necessary, and little room for input from citizens, legislators, data protection authorities or civil society.

When there are limitations on access to information for police, judicial, and other "competent authorities", the principles of availability and mutual recognition permit the continual chipping away at safeguards on individual data protection and privacy, in the name of enhanced cooperation and supposedly more efficient law enforcement. The priority given to increasing the powers of police forces and other law enforcement authorities not only gives impetus to the bypassing of fundamental rights provisions, but also prevents discussion on the causes of crime and inhibits the development of policies designed to create less fractious societies.

It is vital that national parliaments, the European Parliament, individuals and civil society groups call for a complete reappraisal of the approach to police and judicial cooperation in the European Union, and the establishment of systems of cooperation that treat individual rights not as obstacles to information exchange, but as they are intended - principles designed to protect individuals from abuses of state power. The Stockholm Programme and the disproportionate nature of the ECRIS, the EPRIS and the IXP make it clear that such concerns are far from the minds of the EU's policy-makers when plans for enhanced police and judicial cooperation are formulated.

September 2011

To keep up to date see: Observatory:
http://www.statewatch.org/observatories_files/informationexchange_observatory/index.html

© Statewatch ISSN 1756-851X. Personal usage as private individuals/"fair dealing" is allowed. We also welcome links to material on our site. Usage by those working for organisations is allowed only if the organisation holds an appropriate licence from the relevant reprographic rights organisation (eg: Copyright Licensing Agency in the UK) with such usage being subject to the terms and conditions of that licence and to local copyright law.