Interoperability of Police Databases within the EU: An Accountable Political Choice?

PAUL DE HERT and SERGE GUTWIRTH

ABSTRACT This article discusses the interoperability of police databases in the EU with reference to the 24 November 2005 Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs. The different levels of interoperability are identified. Straightforward interoperability within the EU is distinguished from four more controversial levels of interoperability, such as interoperability with atypical systems and interoperability with systems outside the EU. On the basis of this analysis the question of the desirability and suitability interoperability is addressed, followed by a discussion of the necessary guarantees to be included. Contrary to what is often suggested, interoperability is a highly sensitive political issue. The attempt of the Commission’s 2005 Communication, to make it look like a mere technical issue does not create the right context for a serious and in-depth discussion.

Introduction: The Modest Success of Current US and EU Interoperability Programmes

In January 2006 the New York Times published a negative review of the data gathered by the National Security Agency (NSA)—telephone numbers, e-mail addresses and names—and sent to the FBI in search of terrorists. Under strict anonymity some FBI officials complained about the amount of work needed to analyse these data and their lack of value. They also repeatedly criticised the NSA, which was collecting much of the data by eavesdropping on some Americans’ international communications and conducting computer searches of foreign-related phone and Internet traffic, because the unfiltered information was swamping investigators. These comments from law enforcement and counter terrorism officials on the NSA programme do strikingly contrast with the position

Correspondence: Paul De Hert, Tilburg Institute for Law and Technology and Society (TILT), Postbus 90153, 5000 LE Tilburg, The Netherlands. E-mail: paul.de.hert@uvt.nl

ISSN 1360-0869 print/ISSN 1364-6885 online/06/01–2021-15 © 2006 Taylor & Francis

DOI: 10.1080/13600860600818227
of politicians who depict the eavesdropping program as a ‘vital tool’ against terrorism (Bush) having saved ‘thousands of lives’ (Cheney). They also contrast with the impressions of the intelligence officials of the NSA. Rightly the New York Times article observes that the differing views of the value of NSA’s foray into intelligence gathering in the USA may reflect both bureaucratic rivalry and a culture clash. The bottom line seems to be that drawing a clear link between a particular source and the unmasking of a potential terrorist is not always possible. Nevertheless, the intelligence community supported by politicians believes this kind of work is needed.3

The 2005 summer edition of Statewatch provides some European examples that go along with this US story. In one article Martina Kant4 discusses a classified report of the Federal Crime Police Authority (Bundeskriminalamt—BKA) discussing a post 9/11 nationwide data-trawling operation based on profiling (Rasterfahndung), which has led to the collection and classification of personal data from around 8.3 million people. This information included data on people holding flight licenses, flight students, users of flight simulators, members of flying associations, customers registered in the customer database of a company distributing aeronautical supplies, foreign students having followed language courses at the Goethe Institutes; license holders authorised to transport dangerous goods and airport employees, nuclear power stations, 24 chemical companies, the German railway, biological laboratories and research institutes; police data gathered from the national police database (INPOL system) and information gathered from police searches of the ‘Taliban offices’ in Frankfurt/Main in February and June 2001. Although this 20-month long database trawl project was not successful, producing only dry leads (and eventually being stopped),5 it received political backing from the organising agencies and responsible police and interior ministers.6 The Bundeskriminalamt even wants to continue such kinds of data gathering operations and proposes more interoperability between the different security and police services. Martina Kant questions this proposal on cost in terms of resources and data protection principles, and refers to massive civil liberty expenses.7

In the same issue of Statewatch, Marei Pelzer furnishes additional elements to this critical stand on interoperability between secret services and police in her discussion of the new German Immigration Act,8 which came into force on 1 January 2005. The Act enforces a long existing practice, namely, the obligatory requests for information from the internal security service (Verfassungsschutz) on persons before their naturalisation. Pelzer makes the following observation: ‘In practice, the automatic information request from the Verfassungsschutz leads to naturalisation procedures dragging on even more. Security relevant findings almost never appear or are of no substance. The security examination particularly leads to suspicion on the part of the migrant: for people that, in some cases, have lived in Germany already for several generations, the naturalisation procedure has become even more unattractive.’9

Interoperability of Justice and Home Affairs Databases: An Old Idea but a Central Issue Today

The Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 200510 narrowly defines ‘interoperability’ as the ‘ability of IT systems and of the business processes they support to exchange
data and to enable the sharing of information and knowledge’. Henceforth, interoperability is seen as ‘a technical rather than a political concept’. The Commission assumes that the technical dimension of interoperability can and should be disconnected from its other dimensions. For the time being, however, there is no stabilised definition or description of interoperability. As James Backhouse noted, the term ‘only recently crept into our consciousness and as yet finds very few entries in dictionaries and books of reference’.11 Certainly, the rising of the issue of interoperability has been triggered by the launching and development of ‘e-initiatives’ (such as eGovernment and eHealth), which demand smooth and easy communication between all the concerned actors (services, businesses, customers, citizens, etc.). It is also clear that the question of interoperability has been raised in respect of many policy fields as identified by a survey carried out by Kubicek and Cimander: state and society (eParticipation, eDemocracy); social affairs (health pensions, social security); education, science and research; economy and labour; infrastructure; taxes and customs; and police, security and justice. 12 However, it appears that interoperability is a complex issue involving several layers and dimensions, which make its definition a difficult affair, because it bears the risk of strong bias and the generalising of just one perspective. Interoperability is much more than interconnecting ICT-systems. It obviously has technical, semantic, social, cultural, economic, organisational and legal dimensions. That is why Wallwork and Baptista refer to a holistic notion of interoperability, avoiding the pitfalls of a too limitative or too biased definition. Such a notion ‘can serve as an umbrella, beneath which can exist many disparate but complementary definitions, according to perspective or layer of abstraction’.13

The definition proposed by the 2005 Communication is a perfect counter-example of this cautious approach. From the outset it reveals the Commission’s deliberate choice to reduce the scope of interoperability to technical matters and thus stress upon reaching the objective of an accurate and efficient connection of existing systems and available data. It explicitly disconnects the technical and the legal/political dimensions from interoperability, assuming that the former are neutral and the latter can come into play later or elsewhere. This way of proceeding has also been criticised by the European Data Protection Supervisor: it leads to justifying the ends by the means.14 Indeed, technological developments are not inevitable or neutral, which is mutatis mutandis also the case for technical interoperability. Technologies are interwoven with organisation, cultural values, institutions, legal regulation, social imagination, decisions and controversies, and, of course, also the other way round. This means that technologies cannot be considered as faits accomplis or extra-political matters of fact. On the contrary, they are matters of concern or ‘issues’ and require a political state of affairs to be made.15 In respect of interoperability this implies that technical success (‘it works’) cannot be the decisive, let alone the only criterion. It represents only one of the many dimensions of the issue next to its social, cultural, legal, organisational and semantic dimensions. Interoperability issues thus demand an approach that articulates different logics and concerns, dependent from the context or policy domain in which they are raised. This means that questions of interoperability must be contextualised within functions of their possible application fields. In this article, we limit ourselves to interoperability in the context of police, intelligence and justice.

Interoperability of police databases is not a new feature within the justice and home affairs realm. Already by 1977 H. Herold had defended a plan to transform existing police and judicial databases in Germany in one unique system providing information to police and public prosecutors and other services of ‘justice’.16 Although the idea is
not new, technological advances and cost reduction make interoperability a central issue today. The International Civil Aviation Organization (ICAO) mandated the choice for the standardised use of facial recognition technologies for issuance and inspection of machine-readable travel documents and made global interoperability for identification (key-interoperability) a reality. Interoperability also benefits consumers and citizens. Search engines such as Google and Yahoo help us to find our way through the enormous amount of information and data on the Internet and hence ‘enable the sharing of information and knowledge’. They became indispensable interoperability tools, which are so far free of charge. However, these search engines also ‘enable the sharing of information and knowledge’ on persons. Information available on the web on persons is easily gathered. A simple search command does the job. Moreover, by collecting click streams, digital identities of users of the web are created. Specialised firms enrich this information by detecting patterns of consumption on the basis of these click streams, making it possible for commercial firms to bring their advertisements to the consumers that meet their commercial profile. John Battelle holds that net users are only just beginning to come to terms with the trust they transfer to firms such as Google, Yahoo and others to properly safeguard often deeply personal information. Of course, law enforcement and intelligence agencies know about the benefits of search engines. A net search will often be the beginning of an operation. It is well known that net service firms and search engines do hand over records to law enforcement agencies that need the data for ongoing criminal investigations. In many cases data found in computer memory caches or searches people have made online have been used in successful prosecutions.

Safeguards for Acceptable or Ordinary Interoperability within Justice and Home Affairs

According to Herold, access to and sharing of each others information in the justice realm should be governed by three guidelines or guarantees:

1. Sharing should only be possible for law enforcement purposes;
2. The receiving party can only ‘get’ the information when he or she uses it for the purposes that have initially led to its gathering by the sending party;
3. The general principle of efficiency in state administration practice.

Combined with the duty to professional secrecy of all law enforcement authorities in Europe, these guarantees or guidelines provide for a rough but adequate framework for the issue of interoperability. These basic interoperability guarantees must however, as has also been argued by the European Data Protection Supervisor be supplemented with the more refined requirements or principles of the current data protection framework in Europe (infra).

As long as the rough and finer principles are respected, there is no obvious legal problem with the issue of interoperability of police databases, especially because up to now the generic data protection rules set out in the Directive 95/46/EC are not applicable to processing related to third pillar activities of the EU. European data protection was tailored to enable technological and European processing of data, having in mind the model of firms allocating some of their processing work to one Member State and other work to other Member States. Police and justice work today is understood along the same lines. It is almost futile to resist this development. Undeniably European governmental power will
increase with law enforcement authorities becoming more all-knowing through interoperable ‘European’ systems that work on the basis of the principle of availability. If interoperability is refused to these services, each functional within their state borders, then the obvious solution will be created by establishing one European police force with one huge information system. Of course, this option creates different power-concerns, but whatever kind of solution is created, clear and uniform criteria are needed for the enrolment of processing of personal data in European police databases. For example, in the context of the Schengen database, third country residents are refused access to Europe or are refused a visa as a consequence of differences in the criteria applied in the Member States. The existence of such differences between criteria to register people in European databases is an open invitation to discrimination and excessive discretion. It is an obstacle for effective control by national judges.

One possible approach to remedy the negative consequences of the Europeanisation of police databases is to submit these databases to an adapted (and necessarily truncated) data protection framework, which would among others enhance citizen’s rights with regard to police data processing. The proposed framework decision on data protection in the third pillar should be understood in this light. The political debate regarding this important document has not started yet. Many useful suggestions have yet been made by the European Data Protection Supervisor. The current proposal is by all definitions a compromise. The chapter on ‘Judicial remedies and liability’ for example could have been drafted more sharply. Effective protection against the negative consequences of European administrative power demands a swift effective remedy. The judiciary should have effective means to protect (and restore) the rights of the individual.

Interoperability of Justice and Home Affairs Databases: More Controversial Applications

Although the interoperability of police and justice databases will be realised technically, it must be sanctioned legally after the decision concerning the sensitive political debate on the question ‘How all-knowing do we want police to be?’ The political attention should therefore shift to interoperability issues that in some way or another create problems with regard to guarantees identified above, especially with the three ‘rough’ guidelines already identified by Herold in 1977. We identify four sensitive and controversial applications of interoperability, each of which creates specific risks.

1 Interoperability with Systems Outside the EU

The sensitivity of this issue is self-evident. Where privacy protection with regard to police data within the EU is (in practice) mainly the result of the closed nature of police database systems, there is no basis to assume these practical and legal guarantees are respected outside the EU. Even with countries that have reached a comparable level of adequate data protection, there is still a problem of effective legal remedies and control. Non interoperability should therefore be the rule. An exception can only be allowed for restricted interoperability in certain well-defined cases for restricted purposes and on the basis of reciprocity. In practice this means no common technical platforms, no (more) global interoperable keys, no global principle of availability, but exceptional ad hoc transfers of data between police forces in respect of the principles laid down in agreements on
criminal cooperation and data protection regulations. With regard to the latter we refer to the relevant chapter in the proposed framework decision on data protection in the third pillar and the comments made by the European Data Protection Supervisor in his opinion.\textsuperscript{30}

2 Interoperability not of Content but of Keys

A distinction can be made between interoperability of keys and interoperability of content. Traditionally content is made accessible by using alphanumeric data such as names and/or date of birth. Because of problems with spelling and accuracy, the creation of unambiguous identifiers (e.g. biometric data and social security numbers) is considered to be a necessity by many. The 2005 Communication calls for interoperability of national DNA and fingerprint databases to identify persons for whom only biometric information is available (e.g. a photo, a fingerprint or a DNA code). Concurrently, the Communication regrets the limited scope of the current SIS II improvements that ‘only allow for the introduction of an alert if at least basic alphanumeric information can be entered in the system’ and refers jealously to the Prüm Treaty that already allows for the exchange of biometric data.\textsuperscript{31} However, we observe that the Prüm Treaty introduces safeguards for the transfer of data collected. Article 2.2 provides that ‘reference data shall only include DNA profiles established from the non-coding part of DNA and a reference. Reference data must not contain data from which [the] data subject can be directly identified.’ Further, ‘the data subject shall be entitled to have inaccurate data corrected and unlawfully processed data deleted’. Article 40 finally provides that ‘the Contracting Parties shall also ensure that, in the event of violation of his rights in relation to data protection, the data subject shall be able to lodge a complaint to an independent court or tribunal within the meaning of Article 6(1) of the European Convention on Human Rights or an independent supervisory authority within the meaning of Article 28 of Directive 95/46/EC’.\textsuperscript{32}

Today large-scale applications are implemented on both sides of the Atlantic. At a public hearing in the European Parliament on 2 March 2004, European Justice and Home Affairs Commissioner António Vitorino said appropriate use of biometrics would dramatically improve identification and protect citizens from ID theft. The Commissioner highlighted the successful work of the EURODAC fingerprint database for the comparison of fingerprints of asylum applicants and illegal immigrants, saying that out of 250,000 identifications there has not been one ‘false positive’ ID.\textsuperscript{33}

However, this technical shift towards key-interoperability is not evident and there is much concern about premature introduction of biometric identifiers. All unique identifiers, including biometric applications have an error-rate that is undesirable when working with large-scale applications. Some biometrical applications are still in an experimental phase, for instance the use of video surveillance at airports combined with ‘face recognition’ technology to check identities against photographic databases of criminal suspects. Even when one assumes that advances in technology may improve the record of this technology, the fact remains that terrorists will not line up to let their picture be processed in the system. In the same way, ID cards will be forged, purchased from corrupt officials or simply obtained using other documents that are themselves false. Existing business practices to facilitate border procedures for persons with such a card are an open door for terrorists to step in. The ID cards will not help to identify terrorists before they strike.\textsuperscript{34}
Biometrical operability or numbers operability also creates a false promise of efficiency. The examples above show a high degree of 'noise' within the collected data. Unique identifiers may help in limiting the filth at the moment of identification, but they cannot limit the amount of filth behind the identifiers. Also, there is a constitutional or human rights problem with unique identifiers in some Member States (e.g. Germany where a personal identification or registration number (PKZ) was declared unconstitutional by the Federal Constitutional Court) and there is resistance against their use in the privacy community. Enhanced key interoperability is simply not a desired good for many. A privacy-decent border is trespassed and a level of transparency of citizens is made possible that is problematic in a democratic state keen on power management. Nevertheless, there are indications that this cultural resistance can be met or can be circumvented. Globalisation and enlargement is one factor that comes into play. The decision to include mandatory fingerprints in EU passports was defended by Vitorino with the argument that in his Member State people were used to fingerprinting. So why not the rest of Europe?

In his comment on the proposed framework decision on data protection in the third pillar, the European Data Protection Supervisor observes that neither the proposed framework decision, nor the proposal for a Council framework decision on the exchange of information under the availability principle address the sensitivity and specificities of biometric data and DNA profiles from a data protection point of view. This good suggestion is followed by some general recommendations.

Key interoperability is certainly not an uncontroversial topic, it is at least as sensible as interoperability of content. To create key operability is a political choice. To create non-mediated or privacy-unfriendly key operability is a second political choice, to be distinguished from the first. In our former work, based on a legal and ethical assessment we opposed the view that data protection will do for biometrics. Data protection rules need to be supplemented with incriminations for theft and unauthorised use of biometric data and prohibitions on unnecessary or risky use, e.g. for ordinary financial transactions (as opposed to, say, access to ATM machines), for social benefits or employment, or for potentially dangerous uses such as “keyless entry” into hotel rooms; prohibitions of multi-model biometrics; prohibitions of central stored biometrics; prohibitions of storing “raw images”; prohibitions of using financial rewards to promote participation in biometric identification programs; prohibitions on non-encrypted processing and transmitting of biometrical data; prohibition of biometrical technology that generates sensible data when alternatives exist.

3 Interoperability Between Law Enforcement Systems and Other Systems

A third controversial aspect of interoperability surfaces when systems and processes are linked with police databases that are not serving law enforcement purposes. The controversial aspect regards both the use by law enforcement authorities of other state held databases and their use of databases held by non-public actors. The main problem here is not so much ‘abuse’ but trust.

Students learning German at the Goethe Institute do not expect to be enrolled in anti-terrorism profiling programs. For some, this observation settles it: there is not one good reason to process data about students in a law enforcement context. Others remain doubtful: what is so bad about this, granted that it is done for law enforcement purposes? The main problem with trust as one of the core objectives of data protection is its understanding. Simple explanations rarely provide full understanding. In a democratic liberal
state policy makers have an enduring responsibility to take the issue of trust seriously and to create the conditions under which trust can permanently and interactively be reconstructed. There is not one single ‘good’ in a society, e.g. security. There is a plurality of values that do not always coincide and often conflict. European data protections recognise this in different ways: by identifying and distinguishing categories of sensible data that are submitted to tougher rules; by imposing the collection limitation principle according to which there should be limits to the collection of personal data and such data should be obtained fairly and lawfully and, where appropriate, with the knowledge or consent of the data subject; or by enforcing the purpose specification principle and the use limitation principle. A strict interpretation of these principles explains the rather rigid rules on communication of police data to other public bodies and to private bodies laid down in principles 5.2 and 5.3 of the Council of Europe 1987 Recommendation No. R(87) 15 regulating the use of personal data in the police sector.

Legally speaking, these principles can be accommodated easily by governments. It is often remarked that European data protection is too soft for governmental desires. A simple law allows for police powers to demand disclosure for purposes other than those first specified, but the political problem remains. Interoperability, made possible by law, disrespects the importance of separated domains and cuts through their protective walls. The use limitation and purpose specification principles are put aside. Data, gathered by some, are used by others for purposes that were never to be foreseen at the time of their gathering. This is all the more problematic because the purpose specification principle is at the heart of data protection according to which the processing of personal data is not banned in a principled way, but allowed on the condition that the processing meets specified, explicit and legitimate purposes. The idea that the separation of powers is a good way to keep those powers in check lies at the core of the purpose specification principle. Because the power of the processors and the ability to influence behaviour expands with their increase in exchanges, sales, linkages, groupings, analyses and availability of personal data, their competence to process is limited to meet well-defined goals. In other words, processing operations are not banned but must be separated. From that perspective interoperability of data processing becomes not only a very complex, but also a highly fundamental and symbolic case.

From this perspective the Treaty of Prüm and documents such as the 2005 Commission Communication, creating new interoperability powers and calling for more interoperability, disregards the values at the core of data protection: making data processing possible avoiding excessive concentration of controlling power and the total transparency of individuals. Of course such initiatives are inspired by the conventional wisdom in the security field that ‘more is better’ and that an increase in the number of databases increases security. In other words, one policy aim, one good, for instance security, is taken as an absolute. Questions about the necessity of trust based on the idea of the plurality of societal goods, translated into data protection as the purpose specification principle, are left unanswered.

The idea of interoperability should be implemented with care and respect for the plurality of the values and the polyphonic nature of our states. In a democratic constitutional state no policy should be exclusively instrumental to one objective, be it security or anti-terrorism. There are always balancing interests. Moreover, citizens have to deal with government for a number of very different reasons. It would be disrespectful of the ideas behind data protection to see government as a whole that may use ‘its’ information, taken at random from whatever governmental database, let alone from private databases.
Just as the checks and balances of the separations of powers, limited interoperability is to be the rule. Exceptions (immediate or unmediated interoperability) should thus be carefully assessed in the light of the rules and the rationale between the existing (separated) domains. The goal should be an intelligent police, not an all-knowing police with naked citizens. In the same way that telephone companies cannot decide to intercept the telephone conversations of their clients, police forces should not be allowed to establish interoperability. The balancing of interests at stake with interoperability demands should always be done at a higher level and under judicial control.\textsuperscript{42} A prior checking can be entrusted to data protection authorities or, and this option has our preference in view of avoiding bureaucracy and not compromising the independence of the data protection authorities, to an internal body with sufficient guarantees in terms of independence and sufficient expertise in the field of justice and police work. The Europol Treaty with its special regime for working files contains a good blueprint of the system of guarantees that we have in mind. Interoperability should only be possible within a clear legal framework. The ‘bodies’ should be consulted whenever there is a need to create interoperability that is not tied to specific criminal investigations by law enforcement organisations. Questions that have to be considered when dealing with interoperability demands are: Interoperability for what purpose?; What kind of data will be used? What is their source? What use will be made with the results? What guarantees are built in to prevent those who are wrongfully affected becoming stigmatised? In the line of the 2005 Commission Communication we observe that the when considering these questions, a strict application must be made of the principle of proportionality.\textsuperscript{43} In practice this could imply a prohibition of routine access for law enforcement to non-police databases, such as the VIS.

Articles 13 and 14 of the proposed framework decision on data protection in the third pillar lay down a series of requirements to be fulfilled in cases where personal data are further transmitted to private parties and non-law enforcement authorities. Although the European Data Protection Supervisor considers the additional conditions laid down in these articles to be sufficient, he rightly notes that nothing in the proposal is said about personal data also being transmitted or made available by private parties to law enforcement and judicial authorities.\textsuperscript{44} He recommends that common standards of data protection should apply on access by law enforcement authorities to personal data held by private parties, so as to ensure that access is permitted only on the basis of well-defined conditions and limitations. In particular, access by competent authorities should be allowed only on a case-by-case basis, under specified circumstances, for specified purposes, and be under judicial control in the Member States.\textsuperscript{45}

4 Interoperability within the Framework of Intelligence Led Policing

A fourth controversial aspect of interoperability is related to the turn towards intelligence led policing in recent years. The difference with proactive policing is a difference of degree. Whereas the latter uses so-called soft information (non-verified information often based on interceptions, informers, open sources), the former uses all available information and techniques of crime analysis (such as the use of profiling). It is not hard to see why interoperability serves the purposes of this model of policing.

The concept of intelligence led policing originates from British experiences with combating organised crime.\textsuperscript{46} Today it is benchmarked as the way forward for all policing work. In our work we have been critical about the lack of empirical data that substantiates the choice to operate intelligence led policing for ordinary (visible)
crime.47 ‘Intelligence’ is the traditional work of secret services and there are solid constitutional reasons to clearly separate and render impermeable the work of police forces and secret services. It is detrimental for individuals to end up in a police database. It is probably worse ending up in the files of secret services. However, nothing equals ending up in secret service databases that are interlinked with police databases (and vice versa). Then the worst of both worlds are brought together. In the Schengen system a division of labour between police, secret services and other state authorities is reached by carefully establishing limited interoperability regarding the shared Schengen database. However, these careful ‘firewalls’ are questioned, for instance, in the 2005 Commission Communication when it states that the law enforcement community sees the absence of access by internal security authorities to VIS, SIS II immigration and EURODAC data as a shortcoming.

From a perspective of political choices and data protection principles we fear that the speed and the nature of the reforms do not promise well-balanced outcomes. Reference should be continually made to other existing databases and recent steps and innovations. Before complaining about what is not possible with SIS II, it would be worthwhile to first see what SIS II effectively does make possible in terms of interoperability48 and to look for empirical findings about the effectiveness of these and other initiatives. Will new interlinking possibilities and broader use of alert possibilities in SIS II be more effective? Will the new functions give way to more ‘supposition’ creeping into the system and will innocent people suffer repercussions as a result of being associated with certain crimes and certain criminals?

Behind the question of effectiveness also lays the issue of organisational aspects of interoperability. The US example illustrates differences in culture and working methods between the FBI and NSA that are difficult to overcome. The 2005 Commission Communication regrets the ‘under-exploitation of existing systems’ within the EU, but it only contains proposals to enhance technical interoperability. It does not draw the conclusion that law enforcement authorities do not share enough information, but rather that they share it badly.49

We do not share the view that intelligence led policing based on interoperability, profiling, non-selection of data, close cooperation with the intelligence community and availability, are tactics that are a priori inconceivable in a liberal democratic state. There is no indication in this direction to be found in the case law of the European Court on Human Rights.50 The political choice in favour of creation of Europol effectively favours intelligence led policing. Although not all Member States were ready for this kind of policing at the moment of its breakthrough, the creation of Europol is a sign that the EU will push interoperability to an extreme in certain cases. Fed by experiences in Member States such as Germany, it does therefore not come as a surprise that the EU is considering computer-assisted profiling in the fight against crime. However, it is undisputed that these developments depart from the old wisdom that law enforcement agencies should only act on material grounds of suspicion and that their work should be separated from these kinds of intelligence agencies (Trennungsgebot). Therefore, the concerns behind the three basic guidelines for ordinary interoperability (listed earlier) need to be respected to the highest possible extent and supplemented with new guarantees or guidelines where necessary.

Intelligence and soft police data do not belong in multifunctional databases such as SIS and VIS, but should be processed in separated files or databases of which the user is aware that further checking is required.51 In line with what is incorporated in the Europol
Treaty and what we proposed above in subsection 3, the decision to make databases interoperable should be taken out of the hands of the actors concerned and entrusted to an independent expert body within a clear legal framework dealing with an extensive set of questions and adhering to a strict test of proportionality. Also stringent guarantees are needed to protect persons who are not actively involved in crimes.  

Moreover, profiling techniques need to respect the prohibition on automatic decision making as embodied in Article 15 of Directive 95/46/EC. Results of fishing expeditions cannot be translated into immediate police measures, especially so because our examples above show that swift filtering of a small number of ‘suspects’ from vast amounts of data is still not feasible. Profiling always indicates some extremely highly statistical probabilities, but they remain probabilities: they cannot exclude that reality will turn out to be different. Profiles are non-representational knowledge in the sense that they do not so much aim to represent a current state of affairs, but rather aim to predict future behaviours inferred from past actions. They do not describe reality. Hence, intelligence led police actions should be made the object of continuous empirical and political control following the Europol blueprint. They should be properly isolated from ordinary police work in view of harm reduction and reversibility (e.g. by deleting the files as in the German example or by distinguishing data in accordance with their degree of accuracy and reliability, and in particular that data based on facts are distinguished from data based on opinions or personal assessments).

Interoperability of Police Databases: A Technical Idea?

In its 2005 Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, the Commission states that ‘interoperability forms a technical rather than a legal or political concept. This is disconnected from the question of whether the data exchange is legally or politically possible or required.’ Beyond the insight that such a statement is per se incorrect, because technological developments are never just neutral, and this both from the perspective of their invention and their effects, it is all the more disturbing as concerns police work and thus the power organisation of our societies. Is it acceptable, in a democratic constitutional state, to consider technological promises without taking into account society’s political and legal choices? Do law and politics have to abide by ‘what works’, are they totally instrumental to technology, do they still have a say about what should be reached and through which ways? Is the choice between a family car and a fast sports car a technical choice? Let us ask the average housewife when the average family father comes back from the dealer with the latter.

Experts hold that setting up interoperable systems is a complex operation that goes far beyond the technical interconnectedness of databases and systems. ‘Interoperability emerges from the need to communicate data across different domains for a specific purpose. Transferring the data may represent a technical challenge because of different protocols, standards and so forth. However, the key challenge is with the purpose, use and changes consequent on transferring that data. Changes in data ownership and custodianship have an effect on power structures, roles and responsibilities and on risk. These issues go well beyond the technical dimension into the formal and social spheres.’
The 2005 Commission Communication disregards the political dimension of interoperability and uncritically presents technological changes as an acceptable policy. The communication turns out to be no more than a wish list compiled to serve the interest of one single good, viz. (assumed) efficiency in security and crime fighting. Indeed, it will then not come as a surprise that the 2005 Communication very poorly describes possible civil liberties ‘expenses’ of interoperability and the critical voices about irrelevant findings, stigmatisation of those affected (surveillance, procedures dragging on). It omits useful distinctions between technical, organisational and legal interoperability issues and distinctions between ordinary and more controversial applications of interoperability.

By identifying these distinctions, this article has attempted to enrich the discussion and outline of specific guarantees for the respective applications of interoperability. As said, a rough approach of principles and safeguards (such as Herold’s) should be supplemented with the more refined and ad hoc work of the competent data protection bodies. Interoperability can be an enormous benefit for citizen and law enforcement agencies. However, without the appropriate control in the hands of the data subjects, ‘interoperability could be another weapon in the hands of the surveillance society, unwelcome in a world where privacy is still valued’.57 It is against all common sense political intuition and does not serve data protection interests to create a technical platform for interoperability while postponing political discussion about what kind of interoperability is needed. The non-interoperability and impermeability of many systems in the past has probably served data protection better than many legal rules with the same goal. There is a lot of wisdom in taking seriously the political dimension of technical things.

Notes and References

1 The first author is member of the Tilburg Institute for Law and Technology. Both authors are researchers in the ‘Law, Science, Technology & Society’ Research Group at the VUB (http://www.vub.ac.be/LSTS/, last accessed 6 June 2006), and participate to the EC funded Network of Excellence, The Future of Identity of Information Society (see http://www.fidis.net, last accessed 6 June 2006). The authors would like to thank James Backhouse for his comments on the text.


3 Ibid.


6 ‘The “deterrent effect” and the “investigation pressure” has led to “insecurity” in fundamentalist groups and this is seen as an achievement’ (Kant, ibid, p 21 with reference to P v Prondzinsky ‘Rasterfahndung’ Deutsches Polizeiblatt Issue 6, pp 15–18, 2002, see p 18).

7 Kant, op cit, Ref 4, p 21).


20 Ward, op cit, Ref 19.

21 Herold, op cit, Ref 16, pp 48–49.

22 EDPS, op cit, Ref 14.


24 In the Hague Programme of October 2005 the Commission proposed to substitute the principle that data belong to state authorities (subject of the law to protect the data subject) and can only be transmitted to another Member State on the conditions established by the state that holds the information with the ‘principle of availability’. Under the latter principle, the authorities of any Member State would have the same right of access to information held by any other authority in the EU as applies to state authorities within the state where the data are held. According to the Hague Programme, on 12 October 2005 the Commission made a proposal: see Commission of the European Communities, Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490 final (available via http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0490en01.pdf, last accessed 6 June 2006). This proposal is discussed in EDPS, op cit, Ref 14.


28 Brouwer and Alfenaar, op cit, Ref 25.

29 This article only discusses data protection. In a broader perspective the question of the relationship between interoperability and the legal framework of judicial cooperation in criminal matters should be asked. In brief one can say that this framework based on the legitimate idea of judicial control of all transborder transfers of law enforcement data, has lost much of its importance owing to two reasons. First, the framework does not consider transfer of ‘non-criminal’ police data, viz. data gathered by the police for other than law enforcement tasks, in particular public order related data (e.g. hooliganism). The judicial overview imposed by the said framework is therefore limited. Second, recent treaty making (Schengen, Prüm, etc.) shows a willingness of Member States to replace a priori judicial checking on transfers of ‘law enforcement’ police data by a posteriori judicial checking only in cases where the use of these data leads to criminal proceedings (P De Hert and J Vandenborgh Informatieve politie-samenwerking over de grenzen heen [Cross-border exchange of police data], Uitgeverij Politeia, Brussels, 1996). Third, courts in general have been unwilling to exclude use of evidence obtained with disrespect of the said framework. From a data protection perspective, these elements, especially the second and third factor, have watered down safeguards outside the regular data protection framework that could have been nevertheless of great significance.

30 EDPS, op cit, Ref 27, paras 103–104.

31 ‘The fact that the Treaty of Prüm, signed by seven Member States on 27 May 2005, will introduce an exchange of fingerprint and DNA data on a bilateral basis, pending the adoption of such an instrument at the European level, highlights this gap’ (2005 Communication, op cit, Ref 10, para 4.9). This treaty, concluded without the EU framework, is named after the German city in which it was signed. It has not been published in an official journal.


37 EDPS, op cit, Ref 27, para 80.

38 P De Hert ‘Biometrics: legal issues and implications’ Background paper for the Institute of Prospective Technological Studies, DG JRC—Seville, European Commission, January 2005,

39 H Singer-Dekker ‘Misbruik te goeder trouw van persoonsgegevens’ [Abuse in good faith of personal data], Justitiële Verkenningen No. 6, pp 65–73, 1978 (see p 66).


41 Balzacq et al, op cit, Ref 32, p 15.

42 Singer-Dekker, op cit, Ref 39, p 69.


44 EDPS, op cit, Ref 27, para 114.

45 EDPS, op cit, Ref 27, para 119.


49 Balzacq et al, op cit, Ref 32, p 15.


51 Brouwer and Alfenaar, op cit, Ref 25.

52 EDPS, op cit, Ref 27, para 89.


54 See COM (2005) 475 final, op cit, Ref 26, art 4.1 (d).

55 2005 Communication, op cit, Ref 10, p 3.

56 Wallwork and Baptista, op cit, Ref 13, p 19.

57 Backhouse, op cit, Ref 11, p 1.