EUROPEAN PARLIAMENT

2004 *2009*

Committee on Civil Liberties, Justice and Home Affairs

30.9.2008

WORKING DOCUMENT

on problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Sarah Ludford

1. Introduction

It is a fundamental principle of the rule of law that law enforcement actions should be based on an individual's personal conduct, not on their identity. Thus normally people can only be singled out for investigation or checks on the basis of reasonable suspicion stemming from their own actions. But Member States and law enforcement and border control agencies are increasingly interested in 'profiling' as a technique that may aid in the pro-active identification of groups of people who merit further screening or are considered likely perpetrators of crime and terrorism. Profiling is occurring in the policing and criminal justice system including police stop and search and identity checks, during security checks at airports and other ports of entry, and in the selection of persons for surveillance in counter-terrorist efforts.

This takes place in a context where Europe's rapidly-expanding immigration and border control databases and the increasing exchange of information offer a new information resource for law enforcement and counter-terrorism as well as for immigration control. One form of profiling, commonly termed data mining, is the use of automated searches of databases on the basis of pre-selected criteria that may include (but are not limited to) race, ethnicity, religion and national origin.

This report is being undertaken in the belief that the use of profiling and data-mining justifies a public and parliamentary debate. Insufficient attention has been paid to the risk of discrimination or misuse in the use of sensitive personal information in profiling exercises, and to the need for such actions to be objective, proportionate and necessary if they are to meet legal criteria in European human rights and anti-discrimination law. Profiling can be implicit, for example when it reflects a reliance on stereotypes about minority groups' propensity to offend in police decisions about which persons appear suspicious. Studies have been done to examine the incidence of this in relation to, for instance, Roma people. Other forms of profiling are explicit, as when a specific set of criteria are used as the basis for directing investigative inquiries.

But there is little clarity or consensus as to which practices in fact constitute profiling, to what extent they may be legitimate, and what safeguards are required to prevent illegitimate and discriminatory profiling.[1] The European Parliament has raised repeated concerns related to profiling, in particular regarding race, ethnicity and religion, in the context of data protection, law enforcement cooperation, exchange of data and intelligence, aviation and transport security, immigration and border management and treatment of minorities. However there has been no adequate examination of the legal and other issues which might lead to some agreement on what is acceptable and what is not.

2. Reaching a definition of profiling

There is a need to get some agreement on a definition, then guidance on the legitimacy and legality of specific instances of profiling, as a basis for the creation of safeguards and accountability mechanisms.

There exists no EU definition of profiling, ethnic or other, nor any consensus as to the range of practices and actors that it might encompass. The lack of conceptual clarity inhibits the

[1] We should also be aware that profiling based on nationality can be a proxy for ethnic profiling.

debate. There have been two somewhat distinct approaches to defining profiling in the European context: one approach emerges from a data protection perspective, while the second is offered from an anti-discrimination perspective.

Two definitions from the data protection perspective are:

> "A computer method making use of data mining on a data warehouse enabling or intended to enable the classification with some probability -and thus some margin of error- of an individual in a specific category in order to take individual decisions towards that person."[1]

> "The process of inferring a set of characteristics (typically behaviour) about an individual person or collective entity and treating that person/entity (or other persons/entities) in the light of these characteristics."[2]

These definitions view profiling as a neutral process of investigation, omitting consideration of the consequences of using sensitive personal data and the risks of discrimination. Nor do they establish law enforcement as the critical arena in which profiling is a cause for concern as to its potential discriminatory impacts.

Other definitions are grounded in an anti-discrimination perspective and concentrate on ethnic profiling:

> "The use by the police, with no objective and reasonable justification, of grounds such as race, colour, language, religion, nationality or national or ethnic origin, in control, surveillance or investigation activities"[3]

> "[Ethnic profiling is] the use of ethnicity, race, national origin or religion, rather than individual behaviour as a basis for making law enforcement and/ or investigative decisions about persons who are believed to be or to have been involved in criminal activity."[4]

> "[Ethnic profiling is] the practice of using 'race' or ethnic origin, religion, or national origin, as either the sole factor, or one of several factors in law enforcement decisions, on a systematic basic, whether or not concerned individuals are identified by automatic means."[5]

3. Scope of profiling: counter-terrorism, law enforcement, immigration, customs and

[1] See the recent study of the Council of Europe on profiling.
[2] L.A. Bygrave, Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling, *Computer Law & Security Report*, 2001, vol. 17, p. 17-24
[3] European Commission against Racism and Intolerance (ECRI) General policy recommendation No 11 on combating racism and racial discrimination in policing, adopted on 29 June 2007, CRI/Council of Europe (2007)39, paragraph 1.
[4] Presentation by Rebekah Delsol, Open Society Institute to the LIBE Round Table: "Liberty and Security in Integrated Management of EU Border", Brussels, 30 June 2008.
[5] De Schutter, Oliver and Ringelheim, Julie (2008), "Ethnic Profiling: A Rising Challenge for European Human Rights Law," *Modern Law Review*, 71(3):358-384.

border control

Profiling is used in many different fields of law enforcement and administrative control, ranging from counter-terrorism[1] and domestic law enforcement to immigration, customs and border control. The lines between these different fields have become increasingly blurred as information collected in one area is shared with others, as agencies respond to pressures to increase intelligence sharing under the principle of availability, and as broader efforts are made to promote increased cooperation and joint operations. EU databases such as the Visa Information System (VIS)[2], the Schengen Information System (SIS I and SIS II) and Eurodac are viewed as a resource for criminal justice cooperation as reflected in proposals to grant law enforcement access to these data bases and to create operational links between VIS, SIS II and Eurodac.

The Commission proposal for a European Passenger Name Record (PNR) system[3] provides for the collection of the personal data of passengers travelling to the EU. The proposal is for "running the PNR data of passengers against a combination of characteristics and behavioural patterns aimed at creating a risk-assessment". Although the Commission has declined to accept the label of "'profiling' for this activity, a common-sense view suggests it must fit any reasonable definition. A passenger fitting the relevant risk-assessment 'profile' would be identified as a high-risk passenger, and possibly subject to further actions.

The Commission Communication on the creation of an entry-exit system[4] envisages the possibility that domestic law enforcement could use information, including biometric data gathered from travellers entering or leaving the Schengen area in their domestic, non-border, identity checks. It is likely that decision-making in the use of these databases may use profiles based on personal data, including sensitive data. The Electronic System of Travelling Authorisation (ESTA) will "concern third country nationals not requiring a visa [and] allow national authorities to make an individual assessment of each passenger before he/she embarks on an aircraft heading to Europe." However, the process of certifying whether a person is a bona fide/low risk traveller or a threat to public security and order is left to Member States on the basis of undefined criteria. Presumably they will draw up risk assessment profiles as a basis for decisions.

It is alarming that these proposals are moving very rapidly when there is a serious information gap with regard to profiling practices at borders; very few studies exist. In part, this reflects the specific challenges of defining and monitoring profiling in the case of immigration decision-making, which is, by definition, based first and foremost on the nationality and visa status of the person seeking to cross the border.[5] Studies are also hampered by law enforcement reluctance to share investigative guidelines and information on specific practices

[1] Council decision 2005/671/JHA on the exchange of information and intelligence between Member States, 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, in particular as regards serious offences including terrorist acts.
[2] OJ L 218 of 13.8.2008 of 23 June 2008, p. 60 and p. 129.
[3] COM (2007) 654.
[4] Preparing the next steps in border management in the European Union COM (2008) 69, 13.02.08.
[5] Written submission Open Society Institute to the LIBE Round Table: "Liberty and Security in Integrated Management of EU Border", Brussels, 30 June 2008, p. 4.

that use sensitive criteria.

There is, in addition, clear potential for an accountability gap when databases such as the EU PNR and Entry-Exit Scheme are created at EU level but criteria for risk analysis are left up to the Member States. Is there EU competence to ensure that adequate safeguards are put in place?

4. Establishing the legality of profiling

Profiling may be indisputably legitimate, for instance in the development of profiles to support criminal investigations, such as "suspect profiles" that describe a particular person or persons being sought for a particular crime at a particular time in a particular place. Such suspect profiles may also pertain to groups, where the there is a demonstrated link between the ethnicity or national origin of organised crime groups or gangs, and this link is grounded in concrete, specific and up-to-date intelligence.[1] In these cases, the use of ethnicity or other personal factors as identifiers is a legitimate law enforcement tool.

But profiling in its various forms may infringe a range of rights under the European Convention on Human Rights including the right to privacy, freedom of movement and religion and non-discrimination. Article 14 prohibits discrimination in the enjoyment of the rights protected by the Convention. Under that standard, if two similarly situated individuals are treated differently in the absence of an objective and reasonable justification, one of them has been subjected to unlawful discrimination.[2] ECHR case law has established that where race constitutes an *exclusive* basis for law enforcement action, it amounts to prohibited discrimination. Ethnic profiling practices must pass three scrutiny tests if they are to constitute a legitimate difference of treatment that does not constitute discrimination: effectiveness, proportionality, and necessity.

Directive 2000/43/EC, the Race Equality Directive, establishes in EU law the principle of equal treatment between persons irrespective of racial or ethnic origin.[3] It applies in regard to access to goods and services[4]. The preamble says that discrimination may undermine the EU objective of an area of freedom, security and justice[5], leading some to claim that policing and law enforcement constitutes a 'public good and service' which should therefore come within the scope of the Directive. The reference might indeed suggest that the application of the race equality directive to law enforcement activities is not excluded.

---

[1] Written submission Open Society Institute to the LIBE Round Table: "Liberty and Security in Integrated Management of EU Border", Brussels, 30 June 2008, p.2

[2] Timishev v. Russia, App. Nos. 55762/00, 55974/00, ECtHR 13.12.2005.

[3] OJ L 180, 19.7.2000, p. 22.

[4] OJ L 180, 19.7.2000, article 3(1)h.

[5] Paragraph 9 of the preamble states: "Discrimination based on racial or ethnic origin may undermine the achievement of the objectives of the EC Treaty, in particular the attainment of a high level of employment and of social protection, the raising of the standard of living and quality of life, economic and social cohesion and solidarity. It may also undermine the objective of developing the European Union as an area of freedom, security and justice." Council directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation (Employment Equality Directive) however states in article 2(5): 'this directive shall be without prejudice to general measures laid down in national law which, in a democratic society, are necessary for public security, for the maintenance of public order and the prevention of criminal offences, for the protection of health and the protection of the rights and freedoms of others.

Even if its applicability to law enforcement action is accepted, an important exception to the protection offered by the Race Equality Directive is created by Article 3(2) which allows differential treatment on ground of nationality. While immigration decisions have to be made on the basis of nationality, this broad exclusion of nationality discrimination leaves a significant gap in protection and can 'mask' forms of discrimination based on race or ethnic origin as supposedly legitimate differences based on nationality. For example, those responsible for immigration control may stop persons who "look foreign", which in practice generally means non-white European appearance. In an increasingly multi-ethnic society, this practice imposes an unfair burden of law enforcement or control attention on minority groups.

5. Data protection issues

Article 15 (1) of Directive 95/46/EC on data protection gives people a right not to be subjected to "decisions providing legal effects.. based solely on automated processing of data intended to evaluate certain personal aspects."

It is suggested that profiling which simply selects people for further checks, without in itself producing adverse or legal effects for them, cannot be harmful to their interests. Thus the Commission proposal for an EU PNR scheme specifies that there must be a further step, presumably an official's assessment of the relevance of an identification based on risk assessment/profiling, before enforcement action takes place:

"No enforcement action shall be taken by the Passenger Information Units and the competent authorities of the Member States only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation."

However, Article 8 of the draft 'third pillar' framework decision on data protection in policing and criminal justice relaxes that safeguard by providing that an adverse decision can be taken on the basis of data mining or profiling alone, as long as it there is some legal protection for the person concerned:

A decision which produces an adverse legal effect for the data subject or seriously affects him and which is based solely on automated data processing for the purposes of assessing individual aspects of the data subject shall be permitted only when the legitimate interests of the data subject are safeguarded by law.

However, given that no specific standards or criteria are laid down for those measures, the value of this provision appears to be rather low.

Explicit and systematic profiling raises important issues with regard to the protection of personal data, particularly sensitive personal data which is subject to a higher protection standard. Data mining is based on a set of criteria, is often conducted on a large scale, and frequently includes aspects of sensitive personal data such as ethnicity, national origin, religion, of other information that is a proxy for sensitive data (for example, meal choice on flights can identify persons who request halal meals, presumed to be Muslim).

When persons are identified through a process relying on profiling, they are identified as suspicious on the basis of criteria that they have no control to change. In effect, this is akin to a reversal of the presumption of innocence, and points to the need for strong safeguards to protect personal data, particularly sensitive personal data, and restrict the manner in which it has potential for abuse in law enforcement.

European Data Protection Supervisor Peter Hustinx has made clear his view that the proposed framework decision on data protection in policing and criminal justice 'significantly weakens' protection of personal data of European citizens'.[1] As opposed to directive 95/46, the latest draft on which the Council reached political agreement no longer covers domestic processing, and hence would not apply to profiling activities conducted at domestic level.

Other necessary safeguards on the use by law enforcement of personal data include[2]:

- Adequacy and effectiveness: in order for specific profiling practices involving the processing of data to be considered adequate or effective the profile must be based on an objective, statistically significant link between the criteria employed in the profile (ethnicity, age, gender, nationality, etc) and the phenomenon it seeks to address (crime, illegal immigration, terrorism, insurance fraud, etc.).[3]
- Proportionality: the use of the data and the scope of that use must be proportionate to the law enforcement objective to be realised through its use.
- Accuracy: there must be mechanisms that allow for the verification of the accuracy and reliability of personal data entered
- Time limits: the inclusion of a person in a data base must be reassessed regularly, as must the criteria and underlying logic for that inclusion. If there are no valid reasons, the information must be erased. Race, ethnicity and religion do not constitute valid reasons for inclusion in the absence of other material facts.
- Redress: in view of the possible consequences for individuals, redress must be effective and accessible.

6. Discussion and recommendations

The rapporteur hopes that these thoughts stimulate debate about the extent to which profiling is or should be legitimate and legal, and will present recommendations based on discussions within the Civil Liberties, Justice and Home Affairs committee and input from interested parties.

[1] Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27.08.2007.

[2] Contribution by Peter Hustinx, European Data Protection Supervisor, to LIBE Round Table: "Liberty and Security in Integrated Management of EU Border", Brussels, 30 June 2008.

[3] See also European Union Network of independent experts on fundamental rights, CFR-CDF. First report May 2003.