



**DRAFT RECOMMENDATION ON THE
PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC
PROCESSING OF PERSONAL DATA IN THE FRAMEWORK OF PROFILING
Response to Consultation
October 2009**

Introduction:

European Digital Rights is an association of 28 privacy and civil rights organisations based in 18 European countries and active across the European Union. EDRi has observer status to CoE groups since 2005 (Media and Information Society Division) and that we would be willing to be associated in a relevant manner to the work of the CoE services preparing this Recommendation.

In this context, EDRi would also like to draw attention to the principles specified in the recent Civil Society Declaration on “Global Privacy Standards for a Global World” (the “Madrid Declaration”¹) signed by a large number of civil society organisations from around the world.

EDRi feels that the current draft Recommendation underestimates some of the significant challenges that profiling poses for data protection in the online environment. It therefore needs significant alteration before it will be able to achieve its intended goals.

Consent

The Recommendation fails to address how consent (let alone genuinely “informed” and free consent) would be possible in this environment. The practice of profiling is very complicated and becoming increasingly pervasive in the online world. Bearing in mind the sets of data being collected from a whole variety of sources (search engines, advertising “hits”, shopping habits, etc), it is increasingly difficult to imagine the range and importance of the uses and consequences of profiling for individuals. This, clearly, makes the issue of truly informed and free consent very difficult. The difficulties of truly informed consent become significantly greater when data are transferred to third parties. EDRi feels that this issue deserves a great deal more reflection and research into the extent to which adequate information on profiling is provided by online companies and, as a consequence, whether current profiling methods and their consequences are understood and accepted by citizens.

In addition, the issue of free consent must be analysed with respect to the way in which a service or good is used or acquired: in particular, the fact that some services may be used free of charge should not lead to breaches of personal data protection principles and law. The commercial practice of bundling some services and/or goods needs particular attention in this regard. Finally, the Recommendation fails to address the need for increased privacy and personal protection of vulnerable groups of people, first and foremost children and minors. Adequate links or references to other work of the Council of Europe related to this issue could be added to this Recommendation (inter alia those undertaken by the CoE Media and Information Society Division, such as the Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, adopted by the Committee of Ministers on 20 February

¹ <http://thepublicvoice.org/madrid-declaration/>



2008 and the Recommendation Rec(2006)12 on empowering children in the new information and communications environment adopted by the Committee of Ministers on 27 September 2006).

Access to personal data

A significant amount of online data used for profiling are either very indirectly (search engine queries, for example) or indirectly (IP addresses) personally identifiable. This poses a significant challenge for the existing concept of the right to access and rectify personal data. It is therefore not adequate to simply restate existing rights, as has been done in the draft Recommendation.

Discrimination

The document explains, in paragraph 8, that the profiling may suffer from a lack of clarity (or be entirely invisible) as well as a lack of accuracy. Despite this, the document goes on to explain that profiling may be in the legitimate interests of the data subject *inter alia* "allowing the analysis of risk and fraud." An innocent subscriber (or a whole category of subscribers) who is disadvantaged by the risk/fraud analysis being used may have no obvious way of knowing that they are being disadvantaged.

Particularly bearing in mind the accuracy problems mentioned in paragraph 8, it is difficult to reconcile the concept expressed in paragraph 10 that profiling can be in the legitimate interests of the data subject with regard to analysis of risks and fraud with the view in section 3.2 that *profiling must not lead to discriminatory measures of any kind*.

Profiling is done in order to distinguish between different types of behaviour. Citizens are already treated differently on the basis of their location (to limit access for IPR reasons to particular music or video services, for example). It is unclear how this would be seen within the context of the statement that there should not be discriminatory measures **of any kind**.

With regard to the specific text, EDRI has the following comments:

Recitals:

6. Considering that, through this linking of a large number of individual although anonymised observations, the profiling technique is capable of having an impact on the persons concerned by placing them in predetermined categories or groups;

This statement seems to preclude, incorrectly, the possibility of being able to re-personalise such data, even if it has been "anonymised". EDRI feels that this is a significant flaw in the draft Recommendation, which must be rectified.

The issue of re-identification of "anonymised" data is illustrated very clearly by the work of journalists following the leaking of AOL search queries. See, for example:

<http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63>.

This problem is explained in greater detail in this research entitled "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization"

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

A key issue for the recommendation is whether data processing and profiling is being applied in an individualised matter. Although this can be done without a priori identification of the data



subject in the context of online communication technologies, identification of data subjects is typically possible, if needed.

10. Considering that profiling may be in the legitimate interests of both the person who uses it and the person to whom it is applied, such as by leading to better market segmentation, allowing the analysis of risks and fraud, and adapting offers to meet demand; and considering that profiling may thus provide benefits for users, the economy, and society at large, through enhancing the user's experience when surfing the web and delivering more relevant information and services, and that many services, content, and applications on the Internet are largely financed through online advertising;

Such profiling cannot be, in the original sense of the word, "legitimate" unless the legitimate rights of the user with regard to consent, access, information and deletion are maintained. As mentioned above, traditional citizens' rights on these points are significantly challenged by profiling, and further research is needed on this point in order to establish how these rights can be maintained.

Furthermore, it is an unwelcome, dangerous and legally dubious precedent to suggest that certain types of personal data processing are more legitimate because of the uses that the financial benefits may be put to.

Profiling in context of information goods and services, Data on communications and information access behaviour

The Recommendation should clarify, maybe after paragraph 13, that profiling in the context of information goods and services, such as internet access, online newspapers, search engines, social media, online libraries or online bookstores could well have a negative impact on the free exercise of the right to freedom of expression and information. Further research is needed on this point.

18. Considering that the protection of human dignity and fundamental freedoms in the framework of profiling can be effective if and only if all the stakeholders contribute together to a fair and lawful profiling of individuals;

This appears to imply that the citizen is not a stakeholder in this context. There is also a linguistic problem with this text. As it is currently written, it suggests that profiling is needed to protect human dignity and fundamental freedoms.

Definitions

"Profiling" means an automatic data processing technique that consists of applying a "profile" to an individual, namely for the purpose of analysing or predicting personal preferences, behaviours and attitudes

This definition does not cover the use of profiling to identify other attributes such as the geographic location of the data subject (which is not a preference, behaviour or attitude) for the purpose of profiling.

General Principles



3. encourage such individuals, public authorities and bodies to promote self-regulation mechanisms such as codes of conduct ensuring respect for privacy and data protection, as well as develop technologies based on the Appendix to this Recommendation.

It should be made clear in this section that self-regulation and codes of conduct should not be relied upon to ensure adequate protection in this area.

Lawfulness:

4.3 Personal data used in the framework of profiling shall be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed.

The AOL example above shows that this issue is more complex than paragraph 4.3 suggests. There may also be disagreement between what an online provider and a data protection authority may consider to be data that “allows for the identification of the data subjects”. For example, a search engine may feel that IP addresses are not “personally identifiable” because they do not normally identify anyone with the data, while a data protection authority may feel that the *possibility* means that this “allows for the identification” of the data subjects.

The standard “necessary for the purposes for which they are obtained and processed” runs the risk to be entirely meaningless in this context. To better safeguard the final interest of data subject, it would make more sense to say something along the lines of “necessary *and proportionate* for the purposes for which they are obtained and processed *and for which informed consent was given*”.

4.7 The controller shall not use for profiling the data legitimately gathered and processed for other purposes, unless appropriate safeguards are provided.

This paragraph is far too vague. Further processing should not be permitted without an adequate level of informed consent from the individual and, if this is not possible, it does not appear to us that further processing would be legally permissible. The fact that the data will not always be easily identifiable also raises problems with implementation of this provision.

Information:

Section 5.1 should include an option to revoke consent, covering both the initial controller and any persons or bodies to whom or to which the personal data may subsequently have been communicated.

Rights of data subjects:

Section 6.4. *“Unless the law requires profiling in the framework of personal data processing...”,*

It seems premature to include a provision which assumes that it would ever be necessary and proportionate in a democratic society to introduce a law requiring mass automated surveillance (with the ensuing dangers of automated-decision making implied by this) on a scale that appears to be implied under this wording.