

Privacy Platform Meeting
COMPUTERS READING OUR MINDS?

The benefits and risks of profiling

Brussels, 25 January 2012

Profiling - the Council of Europe's contribution

Jörg Polakiewicz¹

Why is the Council of Europe dealing with profiling?

Privacy and data protection have always been **core values of the Council of Europe**. The Committee of Ministers is expected to adopt shortly a Council of Europe Internet governance strategy, which contains a whole chapter on advancing privacy and data protection. Our activities are centred around:

- the **European Convention on Human Rights** (“ECHR”), thanks to which the right to privacy is a directly enforceable fundamental right since 1950, nowadays for 800 million Europeans, and
- the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (**convention 108²**).

On 23 November 2010, the Committee of Ministers adopted **recommendation CM/Rec(2010)13³** on the protection of individuals with regard to automatic processing of personal data in the context of profiling, the first internationally agreed standard in this field. This recommendation is the most recent of several so-called sectoral recommendations adopted on the basis of convention 108.

¹ Head of Human Rights Policy and Development Department, Directorate General Human Rights and Rule of Law, Council of Europe. This article was written in a strictly personal capacity and does not necessarily reflect the official position of the Council of Europe.

²

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=19/01/2012&CL=ENG>

³ <https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM>

Their aim is to ensure that the collection and processing of data in a given sector (e.g. banking, insurance, health, police) or carried out using a particular technique or technology (e.g. smart cards or in our case profiling) are carried out in accordance with the rules and principles of convention 108.

In my intervention, I shall briefly explain the objectives, scope and content of this recommendation.

Objectives

New information and communication technologies (ICT) facilitate the observation and storage of most day-to-day human activities more easily, rapidly and invisibly than ever before, such as buying and selling, searches, reading newspapers, sending and receiving emails. The recommendation underlines that the **increasing use of profiling techniques** poses a **threat to private life**, understood as an individual's capacity for self-determination.

I would like to highlight in particular two risks: **inevitable uncertainty** as to the accuracy of profiles and the conclusions drawn from them and **data decontextualisation**. Since profiling is based on the use of statistics, there is a real probability that a given characteristic will be wrongly attributed to an identifiable or identified individual. In extreme cases, individuals may be deprived from accessing vital goods and services, such as credit or insurance, or may have to pay a higher price⁴ for them. As regards the fight against terrorism, the use of blacklists based on statistical inferences is bound to result in non-terrorists being prevented from boarding planes and offers no absolute guarantee that terrorist passengers will be intercepted.

Moreover, the right to privacy implies the existence of **different spheres of private life** which must be respected by the data processor. Profiling based on data obtained from an individual's Internet use will almost naturally mix data pertaining to separate spheres of private life. Typically, individuals use the same terminal to communicate with their family, employer, friends, doctor, trade union,

⁴ <http://thenextweb.com/>

bank or lover. This means that, in practice, where a general search engine is used, the service provider hosting the search engine has a 'global' view of an identified individual. All this results in what the German Federal Constitutional Court described in its judgment of 2 March 2010 as a **diffusely threatening feeling of being watched** which can impair a free exercise of fundamental rights.

I do not want to be misunderstood in the sense that I would call into question the legitimacy of profiling. As the recommendation also explicitly states, the use of such techniques provides **benefits for users, the economy and society** at large, such as adapting offers to meet demand, permitting an analysis of risks and fraud and assist law enforcement. But the risks mentioned require **effective safeguards against abuse**, which cannot rely only on self-regulation. As the European Court of Human Rights emphasised in many of its judgments, where fundamental values and essential aspects of private life are at stake, state authorities have a duty to establish an effective regulatory and enforcement framework of protection.

Definitions and impact on the right to privacy

The recommendation defines "**profiling**" as an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning him or her or for analysing or predicting his or her personal preferences, behaviours and attitudes, a "**profile**" being a set of automatically generated data characterising a category of individuals that is intended to be applied to an individual.

There are usually **three profiling stages**. The first stage consists of large scale **collection** of usually anonymous data on individual behaviour. This may be a shopping basket, a telecommunications bill or a list of train journeys. During the second stage, data undergo **computer analysis** to correlate certain behavioural characteristics. Invisible to the naked eye, computing power and the

sophistication of algorithms bring to light correlations, without any interference by human logic or common sense. In the third stage, this correlation is **applied to an identified or identifiable individual**.

The recommendation starts from the premise that **individualised profiles** thus generated **are not so anonymous** as sometimes pretended. It covers, even if only incidentally, the collection and processing of anonymous data in as much as the processing of these data in the first and second stages may be crucial in determining the legitimacy and security of processing of personal data in the third stage. In reality, the three stages constitute a continuous process.

Applying profiling techniques, the **web browser editor**, the **cyber marketing company** or a **website** can thus be involved in the processing of personal data. While the information contained in profiles may be considered objective and irrefutable, their processing through automated means allows data controllers to go well beyond neutral identification.

Whenever personal data is being processed, both convention 108 and the ECHR are fully applicable. In **S. and Marper v UK**, the European Court of Human Rights held that, “[T]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of article 8.”⁵ In the online world, the individual contact point (a PC, cell phone or tablet) no longer necessarily requires the disclosure of a person’s identity in the traditional sense. As also recognised by the Court of Justice of the EU, **internet protocol addresses** constitute “**protected personal data**”.⁶

The recommendation’s preamble refers in particular to the linking of a large number of individual, even anonymous, observations, which places people in

⁵ S. Marper v UK, judgment [GC] of 4 December 2008, § 67.

⁶ Scarlet Extended SA v Societe belge des auteurs, compositeurs et editeurs (“SABAM”), Case C-70/10, judgment 24 November 2011, § 51.

predetermined categories, very often without their knowledge. When attributed to a data subject, such profiles make it possible to **generate new personal data** which are not those which the data subject has communicated to the controller or which he or she can reasonably presume to be known to the controller.

Drafting and legal effects

The **committee of experts** established under convention 108 (T-PD) **started its work on profiling in 2008**. The committee is composed of representatives from all states parties to the convention (at the time 41, now 43). Observers from the European Commission, the International Chamber of Commerce and the French speaking association of data protection authorities among others, also contributed to the work with their expertise.

During the drafting process, **public consultations** were held on different drafts of the recommendation and comments were sought from various stakeholders such as Internet access providers, associations of online advertisers and representatives of trade and consumers' associations. The text remained, however, controversial among them, with the ICC opposing its adoption because it considered that it took not sufficiently into account the technological and business reality as well as economic impact and application to various sectors.

On 23 November 2010 the recommendation was eventually adopted by the **Committee of Ministers**, representing the governments of all 47 Council of Europe member states. Only the United Kingdom reserved the right to comply with it or not.⁷ Addressed to the **governments of member states**, it contains **principles and guidelines** to be implemented through national **legislation and self-regulation**. It pursues three main objectives:

- **to provide a coherent normative framework** to be used by national regulators;

⁷ In accordance with Article 10 (2) (c) of the Rules of Procedure of the Ministers' Deputies,

- **to ensure effective protection of the rights of data subjects** striking a **fair balance** between the protection of privacy and the legitimate interests of advertisers and consumers or the public at large;
- **to avoid** that individuals are being **subjected to decisions** – or even worse, **discrimination or stigmatisation** – automatically, on the basis of mere profiles.

Though not a treaty itself, the recommendation deploys certain **legal effects**. Firstly, it must be seen as a further development of the general **principles of convention 108**, applying them to the use of profiling techniques. Secondly, the **European Court of Human Rights** regularly refers to convention 108 and relevant Committee of Ministers' recommendations in its case-law relating to data protection under article 8 ECHR.⁸ The recommendation's standards are thus directly relevant for the interpretation and application of the ECHR.

Conditions

The recommendation starts by requiring member states:

- to guarantee **respect for fundamental rights and freedoms** whenever profiling techniques are used, notably the right to privacy and the principle of non-discrimination;
- to encourage the design and implementation of procedures and systems in accordance with privacy and data protection, already at their planning stage, notably through the use of privacy-enhancing technologies (**'privacy by design'**).

The recommendation further requires that collection and processing of personal data in the context of profiling may only be performed if it is **provided for** or

⁸ See e.g. *S. Marper v UK*, judgment [GC] of 4 December 2008, § 67; *Bouchacourt v. France*, *Gardel v. France* and *M.B. v. France*, judgments of 17 December 2009, §§ 26 and 61.

permitted by law. These references to “law” are of course to be understood not as any law, but legislation in accordance with the principles of this recommendation. Principle 3 (4) (b) for example states that profiling requires the consent of the data subject or must be necessary for the performance of a contract or for vital interests of the data subject or legitimate public interests. Any **consent** shall be free, specific and informed, even explicit in the case of sensitive data.

Today, browser options are configured by default in order to allow **third party cookies**. Does this constitute free, specific and informed consent?

Rights

The recommendation foresees the following **basic rights of data subjects**:

- **to receive information** including on the purposes and effects of profiling. The right to be informed (by consulting on-line newspapers) shall not be interlinked by default with third party observation;
- **to object to the use of their personal data** for profiling;
- **to object to decisions** having legal or other significant effects, including where such decisions are taken in the course of the performance of a contract;
- **to obtain** from the data controller **communication** of personal data, the logic underpinning the processing, significance and consequences of the profiles attributed.

Exceptions

The recommendation allows for exceptions to some of its principles, thus taking a **balanced approach**, which leaves states a certain margin of appreciation. Since such exceptions will constitute restrictions to the right to private life or other rights under the ECHR, the **conditions and safeguards under the ECHR apply**, notably the requirement that such measures must be necessary in a democratic society and satisfy the proportionality test applied by the Strasbourg Court.

Remedies

Domestic law should provide for **appropriate sanctions and remedies**, leaving it however to national legislation to fix precise amounts; e.g. German legislation on scoring enacted in 2009⁹ provides for penalties of up to 300,000 € if the interests of data subjects are harmed through wrongful use of data (processing, profiling) or denial of information.

Data security

Appropriate technical and organisational measures will be required to guard against **accidental and unlawful destruction and loss of data** as well as unauthorised access, alteration, communication or any other form of unlawful processing. The appointment of an **independent person** responsible for the security of information systems is required as well as specific measures to **prevent re-identification** of data subjects through the use of aggregated statistical results.

Conclusion

We are not privacy zealots. The recommendation recognises that **profiling pursues legitimate interests**. But take for example the area of online advertising; there are **so many grey areas** that if the end-users knew about it all, it would make their hair turn grey.

We are convinced that more transparency is in the interest of all. If Internet service providers, research and online advertisement companies care about the long-term success of their business, they should take an active role. This is why the recommendation also promotes **self-regulation**, not as a substitute for, but in addition to, domestic legislation.

⁹ See Section 43 of the Federal law on data protection (BDSG).