Mireille Hildebrandt

Summary. Some of the most critical challenges for ‘the future of identity in the information society’ must be located in the domain of automated profiling practices. Profiling technologies enable the construction and application of group profiles used for targeted advertising, anti-money laundering, actuarial justice, etc. Profiling is also the conditio sine qua non for the realisation of the vision of Ambient Intelligence. Though automated profiling seems to provide the only viable answer for the increasing information overload and though it seems to be a promising tool for the selection of relevant and useful information, its invisible nature and pervasive character may affect core principles of democracy and the rule of law, especially privacy and non-discrimination. In response to these challenges we suggest novel types of protection next to the existing data protection regimes. Instead of focusing on the protection of personal data, these novel tools focus on the protection against invisible or unjustified profiling. Finally, we develop the idea of Ambient Law, advocating a framework of technologically embedded legal rules that guarantee a transparency of profiles that should allow European citizens to decide which of their data they want to hide, when and in which context.

So far, profiling has not been the subject of a coherent, cross-disciplinary knowledge domain. Research is fragmented between computer engineers, social studies, lawyers, mathematicians, and those working on specific applications within for instance medical research, marketing or forensic science. Profiling is often reduced to data mining and discussed in highly technical terms (Fayyad et al., 1996) or from a social theory perspective in terms of semiotic or Deleuzian inquiries (Elmer, 2004; Hildebrandt, 2008). A coherent legal perspective on profiling, integrating privacy and data protection, non-discrimination, liability issues and forensic profiling has not been attempted yet, even if partial analyses have been made within the context of the FIDIS network (Schreurs et al., 2008; Hildebrandt and Koops, 2007; Geradts and Sommer, 2008). For this reason FIDIS has devoted serious attention to the question

---

1 From a legal perspective analyses are often made in terms of the protection of personal data, whereas specific attention to the legal status of profiles, especially group profiles is lacking.
of what profiling actually is, how it can be defined and explained in a way that is easily understandable across different disciplines. This will be discussed in Section 7.1, mainly building on the cross-disciplinary findings of *Profiling the European Citizen* (Hildebrandt and Gutwirth, 2008).

An important domain of research within the framework programmes of the European Commission as well as within industry is what has been coined as Ambient Intelligence (AmI), ubiquitous computing or autonomic computing. One could translate these terms into the idea of a ‘smart’ adaptive environment that requires little deliberate human intervention. Though AmI depends on a series of enabling technologies for its realisation of smart environments, profiling can be seen as the enabling technology, because to make sense out of the ‘tsunami’ of data that is generated by RFID systems and sensor technologies, profiling is essential. In Section 7.2 we address profiling within the context of AmI.

To assess the impact of profiling technologies on the identity of European citizens two notions of identity have been introduced and explored within the FIDIS network, coined by the French philosopher Paul Ricoeur: idem and ipse. Idem (sameness) stands for the third person, objectified observer’s perspective of identity as a set of attributes that allows comparison between different people, as well as unique identification, whereas ipse (self) stands for the first person perspective constituting a ‘sense of self’. Their intersection provides for the construction of a person’s identity. In Section 7.3 these concepts will be further explored and their relevance for democracy and rule of law will be discussed, pointing out that privacy as a matter of boundary negotiations and identity construction necessitates understanding privacy as a private interest as well as a public good.

After having discussed the risks of increased profiling throughout Sections 7.1, 2 and 3, we turn to a discussion of the legal implications. Data protection and privacy rights provide a legal framework that is mostly focused on the protection of personal data. With regards to the kind of threats generated by refined profiling a complementary focus is needed on protection against unwarranted application of profiles. On top of that the legal framework still ‘thinks’ in terms of the technologies of the script, which renders it ineffective in protecting against dangers afforded by the technologies of the digital and the virtual. In Section 7.4 this challenge is taken up in exploring the notion of Ambient Law (AmLaw), i.e., a type of law that is articulated into the socio-technical infrastructure that it aims to protect against.

Section 7.5 provides some concise conclusions.

---

2 The phrase ‘tsunami’ of data was used in The Future Group Report (2008), written by the Informal High Level Advisory Group on the Future of European Home Affairs Policy. ‘The findings and recommendations of the Future Group are meant to be an important contribution and a source of inspiration for the European Commission’s proposal for the next multi-annual program in the field of Justice and Home Affairs’, see the report at p.3.