Risks and issues of individual profiling

Chapter copied from:
https://en.wikipedia.org/wiki/Profiling_(information_science)

Profiling technologies have raised a host of ethical, legal and other issues including privacy, equality, due process, security and liability. Numerous authors have warned against the affordances of a new technological infrastructure that could emerge on the basis of semi-autonomic profiling technologies (Lessig 2006) (Solove 2004) (Schwartz 2000).

Privacy is one of the principal issues raised. Profiling technologies make possible a far-reaching monitoring of an individual's behaviour and preferences. Profiles may reveal personal or private information about individuals that they might not even be aware of themselves (Hildebrandt & Gutwirth 2008).

Profiling technologies are by their very nature discriminatory tools. They allow unparalleled kinds of social sorting and segmentation which could have unfair effects. The people that are profiled may have to pay higher prices,[7] they could miss out on important offers or opportunities, and they may run increased risks because catering to their needs is less profitable (Lyon 2003). In most cases they will not be aware of this, since profiling practices are mostly invisible and the profiles themselves are often protected by intellectual property or trade secret. This poses a threat to the equality of and solidarity of citizens. On a larger scale, it might cause the segmentation of society.[8]

One of the problems underlying potential violations of privacy and non-discrimination is that the process of profiling is more often than not invisible for those that are being profiled. This creates difficulties in that it becomes hard, if not impossible, to contest the application of a particular group profile. This disturbs principles of due process: if a person has no access to information on the basis of which they are withheld benefits or attributed certain risks, they cannot contest the way they are being treated (Steinbock 2005).

Profiles can be used against people when they end up in the hands of people who are not entitled to access or use them. An important issue related to these breaches of security is identity theft.

When the application of profiles causes harm, the liability for this harm has to be determined who is to be held accountable. Is the software programmer, the profiling service provider, or the profiled user to be held accountable? This issue of liability is especially complex in the case the application and decisions on profiles have also become automated like in Autonomic Computing or ambient intelligence decisions of automated decisions based on profiling.

See also

- Behavioral targeting
- Data mining
- Demographics
- Digital identity
- Digital traces
- Forensic profiling
- Identification (information)
- Identity
- Labelling
- Privacy
- Profiling
- Offender profiling
- Social Profile (Social Profiling)
- Stereotype
- User modeling
- User profile