Chapter 17
Concise Conclusions: Citizens out of Control

Mireille Hildebrandt and Serge Gutwirth

For a summary of the contributions we refer to the introductory chapter. In this chapter we undertake to draw some summary conclusions. It seems that profiling, especially in the context of smart applications and Ambient Intelligence, requires a focus shift from data to knowledge, while the type of knowledge that is at stake differs from more traditional knowledge production. We conclude that this shift has far-reaching implications for the relationship between citizens, commercial enterprise and governmental powers. This requires lawyers, policy makers, computer engineers and politicians to rethink the socio-technical infrastructure of constitutional democracy. Citizenship, participation in the creation of the common good and personal freedom cannot be taken for granted, they presume that citizens have some awareness of what is known about them and by whom.

Classification and Profiling

Profiling is a matter of pattern recognition, which is comparable to categorisation, generalisation and stereotyping. To understand what is new about profiling we must differentiate between classification (ex ante categorisation) and clustering (ex post categorisation). Classification is nothing very new, apart from the fact that databases allow more extensive queries; it does not deliver any new knowledge, it only permits a structuration of what was already known. Clustering and association rules, however, produce previously unknown patterns. This means that whoever controls the profiling machinery comes into possession of valuable knowledge and information. This knowledge is statistical and hence, not necessarily ‘true’ or adequating reality but it clearly has an added value.
Non-distributive Group Profiles and Non-universal Categorisation

Similar to non-universal categorisation, non-distributive group profiling reduces complexity without applying to all the elements of the category that is used. As we all know, categorisation allows segmentation and stratification: distribution of risks and opportunities on the basis of being an element in a category. Non-distributive group profiling causes problems whenever a person is categorised in a group while the relevant group profile does not apply. However, this does not mean that correct categorisation is without problems, as this may result in discrimination (if the categorisation is used for unfair distributions of risks or opportunities) or manipulation (if the categorisation is used to influence a person’s behaviour without any awareness on the part of the person).

Data Processing: A Black Box?

The process of data mining is mostly invisible to the individual citizens to which profiles are applied. This is the case because the use of algorithms demands computing powers far beyond the limits of the human brain, requiring machines to do the work. As citizens whose data are being mined do not have the means to anticipate what the algorithms will come up with, they do not know how they will be categorised or the consequences. More complex types of profiling such as neural networks, process data without being able to predict the outcome; in this case the process is a black box even for the programmer and the data analyst. For individual citizens to regain some kind of control over the way they live their lives, access is needed to the profiles applied to them. This will require both legal (rights to transparency) and technological tools (the means to exercise such rights).

Risks and Opportunities

The risks and opportunities of profiling derive from the transparency of the personality, life-style, habits, desires and preferences of individual citizens. Such transparency allows: refined price-discrimination based on refined segmentation; refined criminal profiling, predicting criminal behaviour and/or recidivism; refined targeted servicing, aiming to reinforce or even initiate customers’ behaviour that is profitable to the service provider; refined personalised support for e-learning in schools or workplaces. It should be obvious that these opportunities simultaneously entail risks. The most obvious risk is the inaccuracy of the data used to produce profiles, which may be caused by intentional actions, for instance data minimisation or identity fraud but also by unintentional actions such as human or technical error and the use