January 17, 2008

# Profiling the European Citizen

Serge Gutwirth
Mireille Hildebrandt

**Profiling the European Citizen**
Serge Gutwirth and Mireille Hildebrandt
CPDP2009

Text of the presentation by Serge Gutwirth on 17 January 2009

As you see I'm standing here alone, but, as the program mentions, I speak for two : my presentation has been prepared with two heads and four hands : those of Mireille Hildebrandt and mine.

Mireille and I have had the chance to be the editors of this book *Profiling the European Citizen* published last year with Springer - and which proposes a rich cross-disciplinary collection of contributions and replies on the issue of *profiling*, which we believe to be quintessential for privacy and data protection, today and in the near future.
What follows is thus also indebted to the contributors of the book and to their common work within the European Network of Excellence on "the future of identity in the information" society (FIDIS)

Indeed, it is not possible to do justice to the richness of the research done in 15 minutes, but Mireille Hildebrandt and I will try to present its most striking challenges, conclusions and outstanding issues. We will also suggest some paths to cope with them.

*

As you know profiling can pertain to one individual person, to a group or groups of persons, but also to animals, to objects and to relations between all those.
It can be used, on the one hand, to classify, describe and analyze what happened, which is not particularly new or problematic. In such cases profiling permits a structuration of what was already known.

On the other hand - and this is what we target today - profiling is used to cluster data in such way that information is inferred, and predictions or expectations can be proposed. Such profiling activity thus *produces* a particular sort of knowledge.

The knowledge produced is *non-representational* : it does not represent a current state of affairs: profiles are patterns resulting of a probabilistic processing of data. They do not describe reality, but are detected in data bases by the aggregation, mining and cleansing of data.
Taken to a more abstract level, by mining of machine readable data profiling leads to the identification of patterns in the past which can develop into probabilistic knowledge about individuals, groups of humans and non-humans in the present and in the future.
In a way, our view of present and future is then shaped by what the data mining makes visible.

But indeed even if the profiling process shows that a pattern occurs every time some conditions are met, one cannot be 100% sure it will happen today and tomorrow as well.

> Based on its experience, an animal may associate a situation with a danger as a result of the recognition of a certain pattern and act consistently, even if the situation, in reality, is not a dangerous one : the bad human smell and the shuffling footsteps were not those of a bloodthirsty hunter, but those of a sweet animal rights observer.

The example demonstrates that profiling is not a new phenomenon, but that it is as old as life. It is a kind of knowledge that has always supported the behavior of living beings and humans.

> It might well be that the insight that we often 'intuitively know something' before we 'understand' it, can be explained by the role profiling spontaneously plays in our minds.

The point is, however, that in the recent decades profiling capacities have exponentially grown as a result of both the advances in technology and the increasing availability of readily processable data and traces.
The use and convergence of the web, mobile phones, electronic financial systems, biometric identification systems, RFIDs, GPS, ambient intelligence and so forth, all participate in the automatic generation of data which become available for still more pervasive and powerful data mining and tracking systems.

In sum, an enormous and permanently inflating cloud of electronic dust is there for grabs enabling not only extensive data mining and profiling, but also providing for real-time and autonomic applications which impact upon ongoing actions and their environment.

To us these evolutions represent more than mere quantitative changes. On the contrary, they represent a significant qualitative shift compared to more classical statistical approaches that aim at validating or invalidating already proposed correlations believed to be relevant and pertinent to answer preceding questions. The correlations are the result of an oriented questioning and they are *<u>measurements</u>*.

Today, however, such preceding questions are disappearing. Very differently, the emergence in itself of a correlation has become the pertinent information and will in its turn launch questions and suppositions. Things are going the other way around now: the *<u>detection</u>* of the correlation *is* the information.

Detections, however, are much wider than measurements; they don't have a specific meaning, but they will have an impact if used or applied, and their meaning is produced by their application. In other words, the *qualitative shift* lies in the fact that correlations and profiles get generated before any preceding interest or question.

This is why it can be said humans have become detectable far beyond their control : their actions have become the resources of an extensive, if not unlimited, network of possible profiling devices generating knowledge affecting and impacting upon them.

Indeed, such a shift demands careful monitoring from the perspective of the democratic constitutional state, because it likely entails a number threats to its such as
- the surreptitious influencing, formatting and customisation of individual behavior,
- the sharpening of power inequalities between those that possess the profiles and those that are being profiled
- the making of wrong decisions as a result of false positives and false negatives
- the making of unfair decisions based on correct profiles that allow for unwarranted and invisible discrimination
- and, last but not least, the taking of unmotivated and unilateral decisions about individuals

Next to these threats, profiling is also the precondition for autonomic computing that allows for a new socio-technical infrastructure that 'runs' *autonomically*, that is by taking a number of decisions without human intervention.
Autonomic computing will involve distributed intelligence that emerges from networked objects which are in a process of continuous real time machine to machine communication, and it is not clear how, in the case of harm, liability could be attributed to one of the 'nodes' of such networks. Decisions taken, then, are not intentional in the traditional sense of the word, and they are not taken by one particular human or non-human node. Civil liability can of course be based on a strict liability, but to attribute criminal liability in case where neither a cause nor blame can be attributed we seem to have a problem.
Another issue worth mentioning relates to the legal status of profiles : who has rights upon this machine generated knowledge ? And if someone does, which rights ?

A crucial additional point is indeed that the process of data mining and the ways profiles are build is mostly invisible and uncontrollable for the citizens to which they are applied. Citizens whose data are being mined do not have the means to anticipate what the algorithms will come up with and hence they do not have a clue what knowledge about them exists, how they are categorized and evaluated, and what effects and consequences this entails.

For individual citizens to regain some control, access is needed to the profiles applied to them. This will require both legal tools (rights to transparency) and technological tools (the means to exercise such rights).

> Under the name of "Ambient Law" some - and Mireille to start with - defend the idea that law should be embodied in the socio-technical infrastructure it aims to protect against.

*

From a legal point of view, profiling makes it necessary to clearly distinguish between privacy on the one hand and data protection on the other.

*Privacy* is recognized as a fundamental right in different major international legal instruments and in many national constitutions. In short, it protects a number of fundamental political values of democratic constitutional states, such as the freedom of

self-determination of individuals, their right to be different, their autonomy to engage in relationships, their freedom of choice, and so on.
By default privacy prohibits interferences of the state and private actors in the individuals' autonomy : it shields them off from intrusions, it provides them a certain degree of opacity and invisibility.

> The scope and reach of privacy are underdetermined and it is up to the judges to decide when privacy interests are at stake and when protection can rightfully be invoked. Legislators can also intervene to protect particular privacy interests, for example through the enacting of professional secrets, the secrecy of communications or the inviolability of the home.

*Data protection* is both broader and more specific than the right to privacy.
It is broader because data protection also protects other fundamental rights such as the freedom of expression, the freedom of religion and conscience, the free flow of information, liberty, the principle of non discrimination, individual self-determination ...
But data protection is also more specific than privacy since it *simply and only* applies when "personal data" are "processed". The application of data protection rules does not raise a privacy issue: data protection applies when the statutory conditions are met.
By default, and contrary to privacy, data protection rules are not prohibitive, but they organize and control the way personal data are processed: such data can only be legitimately processed if some conditions pertaining to the transparency of the processing, the participation of the data subject and the accountability of the data controller are met.

With regards to profiling, the former entails that data protection law only applies when profiling activities involve personal data.
Protection beyond personal data is not foreseen and that actually leaves out the situations wherein profiling techniques make it possible to impact upon a person's behavior and autonomy *without* rendering this person identifiable, which will happen frequently, particularly in applications of ambient intelligence.
Nevertheless, in such cases privacy interests are still under pressure and privacy protection can be called upon, which significantly implies that the non-applicability of data protection does not mean that there is no existing protection since privacy can be invoked.

> This indeed is not to say that there is no need for a better protection, considering especially the invisibility of the profiling process and the ensuing profiles. The problem is also that threats to non-discrimination and due process are not really met in the present legal framework.

That is why we think that *"profiling" calls for a system of protection of individuals against the processing of data that impact upon their behavior even if those data cannot be considered as personal data*, which implies a shift from the protection of *personal* data to the protection of data *tout court* ! … It might seem so, but in fact this is not a revolutionary step since it just picks up the tread opened by the Directive 2002/58 which, in order to protect privacy, provided for the protection of location and traffic data (which are not necessarily "personal data").

> Also, the same directive 2002/58 gave us the inspiration to plead for a regulation of ‘unsolicited adjustments’ similar to the existing regulation of ‘unsolicited communications’ or ‘spam’, providing for an opt-in system. No adjustments without explicit prior consent, would then be the rule. I will not elaborate upon this idea since Gloria Gonzalez Fuster will pick it up later during the 11 o’clock panel.

More generally speaking, we should maybe explore the possibility of a new legal approach of profiling, focusing on the way profiles can affect our behavior and decisions. Such a shift would emphasize the issues of discrimination and manipulation of conduct through the use of profiles, as well as the transparency and controllability of profiles.

*

Furthermore, even if data protection law theoretically applies to many facets of profiling, many problems subsist, because its techniques remain a technological black box for citizens, making data protection uneffective and unworkable.
Where data protection demands transparency and controllability, data mining and profiling tend to remain opaque, incomprehensible and evasive.
That is why the integration of legal transparency norms into technological devices that can translate, for the citizen, what profiling machines are doing is a priority.

If we want to anticipate and/or change the way machines profile us, we will need what we have called “transparency enhancing technologies” (or TETs).
If “Privacy Enhnacing Technologies” or “PETs” aimend at technologically enforce the individuals invisibility, “TETs” would involve the integration of legal transparency in the technological infrastructure they aim to protect against. As such they would empower citizens to unfurl the profiling operations they are subject to.
TETs, however, are still to be invented and their application may run counter to the intellectual property rights of the owners of databases, while the question remains how humans could effectively communicate with the machines that provides transparency of the proliferation of profiles. This is a topic presently under investigation within the FIDIS research network.

Profiling is a powerful technique that renders visible what is invisible to the naked human eye. This, however, concerns patterns in data bases that must not be mistaken for reality. By making visible what is aggregated in the data base, profiling also make invisible what cannot be translated into machine readable data.
In as far as the governance of people and things becomes dependent on these advanced profiling technologies, new risks will emerge in the shadow of the real time models and simulations these technologies make possible.
What has been made invisible can grow like weed. Threats to privacy, liberty, due process and non-discrimination may in fact hide under the surface of what has been called ‘hidden complexity’.

We hope that this conference will help to re-visualize what is happening under the sheets of autonomically interacting networks of things and other applications of ambient intelligence, and that it will put profiling on the agenda of policy makers, academics and activists as one of the most powerful and invisible techniques shaping our present and futures.