IDIS (2008) 1:55–70
DOI 10.1007/s12394-008-0003-1

Profiling and the rule of law

Mireille Hildebrandt

Received: 1 March 2008 / Accepted: 25 July 2008 / Published online: 19 December 2008

Abstract Both corporate and global governance seem to demand increasingly sophisticated means for identification. Supposedly justified by an appeal to security threats, fraud and abuse, citizens are screened, located, detected and their data stored, aggregated and analysed. At the same time potential customers are profiled to detect their habits and preferences in order to provide for targeted services. Both industry and the European Commission are investing huge sums of money into what they call Ambient Intelligence and the creation of an 'Internet of Things'. Such intelligent networked environments will entirely depend on real time monitoring and real time profiling, resulting in real time adaptation of the environment. In this contribution the author will assess the threats and opportunities of such autonomic profiling in terms of its impact on individual autonomy and refined discrimination and indicate the extent to which traditional data protection is effective as regards profiling.

Keywords Profiling · Data protection · Social sorting · Privacy · Rule of law · Freedom

Abbreviations

AmI	Ambient Intelligence
BPP	Behavioural Biometric Profiling
CRM	Customer Relationship Management
CTA	Constructive Technology Assessment
DM	Data Mining
HMI	Human-Machine Interface
KDD	Knowledge Discovery in Databases

M. Hildebrandt
Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussel, Belgium
e-mail: mireille.hildebrandt@vub.ac.be

M. Hildebrandt (✉)
School of Law, Erasmus University Rotterdam, P. O. Box 1738, NL-3000 DR Rotterdam, Netherlands
e-mail: hildebrandt@frg.eur.nl

M2M Machine-to-Machine Communication
MAN Multi-Agent Network
PET Privacy-Enhancing Technology
TET Transparency-Enhancing Technology
UST United States Department of Treasury

Introduction: the age of identification[1]

We live in the age of identification. For different reasons both government and business enterprise strive to develop effective tools for repeated identification and authentication. Writers like Scott (1998) in his '*Seeing Like a State*', and Torpey (2000) in his '*The Invention of the Passport. Surveillance, Citizenship and the State*', have described and analysed the insatiable need of the modern state for the registration of its citizens, originally seeking to attribute and implement tax obligations and register for subscription in the national army. The construction of the territorial nation state required the identification of those aligned to the territory and the nation. As a precondition for taxation and subscription it helped in creating the historical artefact of the territorial nation state. Like the introduction of national languages, national clocks and national currencies, the identification of citizens versus non-citizens in fact was a productive process, not merely the recording of a given fact. Building on the 18th century police state the 19th and 20th century welfare state then claims a need to maintain the line between those that are entitled to public benefits and those that have no such right,[2] while it also claims to need identification for the prevention of fraud, crime and unlawful access in general, and for the attribution of liability, whether criminal or tort. E-government and e-health that aim to provide targeted services reiterate this quest for identification, although in this case the identification needed is more sophisticated and resembles what business undertakings seek when they develop targeted servicing and reinvent customer relationship management (CRM).

Business enterprise is less interested in a foolproof registration of the inhabitants of a territory. Its focus is on acquiring relevant data about as many customers and potential customers as possible as part of their marketing and sales strategies. As customer loyalty can no longer be taken for granted, companies develop CRM in the hope of surviving the competitive arena of neo-liberal market economies. At the same time they try to establish which consumers may be persuaded to become their new customers and under what conditions. It seems that they are less interested in unique identification of any particular customer than in a refined type of categorisation that allows them to provide targeted servicing at the right time and in the right place. *Context is all* is not just the key message of adherents to cultural theory. In fact, companies are not just after the attributes of predefined classes of

[1] This article is the revised version of my presentation at the 7th Social Study of ICT Workshop (SSIT7) on 19–20 March 2007 at the London School of Economics. An earlier version was published in the FIDIS In-House Journal.

[2] The original police states originate in 18th century continental Europe, not to be confused with 20th century totalitarian states. Cf. Dubber and Valverde 2006, at 35.

customers and potential customers, but would rather invest in finding out which classes they should discriminate in the first place. This is where profiling comes in.

In this contribution we will look into the impact of profiling on human identity in constitutional democracy. We will argue that the rule of law both presumes and protects human identity as fundamentally *under*determined. This requires us to foster a legal-political framework that both produces and sustains a citizen's freedom to act (positive freedom) that is the hallmark of political self-determination and a citizen's freedom from unreasonable constraints (negative freedom) that is the hallmark of liberal democracy (Berlin 1969). Profiling technologies could threaten the fragile legal-political artefact of the rule of law, by allowing subtle but pervasive manipulation of the freedom to build one's identity in the face of ever-changing circumstances.

To argue this point we will first discuss how sophisticated machine profiling differs from the kind of profiling we do in everyday life (sections 2 and 3). Next we will investigate profiling as the enabling technology for Ambient Intelligence and the 'Internet of Things' (section 4). Since profiling produces knowledge, rather than just data, section 6 will look into the threats posed by emerging knowledge-asymmetries owing to the proliferation of profiling in smart environments. It is these threats that touch some of the fundamental tenets of democracy and rule of law, being the particular mélange of positive and negative freedom that allows citizens to develop their relative autonomy (section 5). To counter such threats the focus of legal scholars and practitioners should be extended from the protection of personal data to the protection against the undesired application of profiles and the creation of transparency rights regarding group profiles (section 7). To exercise legal transparency rights, the technological infrastructure that is being constructed to facilitate smart environments must incorporate transparency-enhancing technologies (TETs). Section 8 will argue why the introduction of privacy-enhancing technologies (PETs) should be complemented with TETs. Section 9 concludes with some closing remarks.

What else is new? autonomic behaviour and autonomous action

Profiling is as old as life itself. Indeed one could say that the difference between living and lifeless material is the fact that living organisms are capable of self-constitution over and against an environment which is constituted as such by the act of self-constitution (Maturana and Varela 1991). In more simple terms: an organism and its environment co-create each other. Profiling is thus a crucial sign of life, because it consists of a repeated identification of risks and opportunities by an organism in its environment (Hildebrandt 2008a). Profiling is the interplay between *monitoring* and *adaptation*: to survive and to celebrate life any organism must continuously adapt itself to changes in its surroundings, while it may also manage to adapt its surroundings to its own preferences (Maturana and Varela 1991). Monitoring one's context in this sense is a matter of *pattern recognition*, of discriminating noise from information. Not all data are relevant or valid. Whether this is the case will depend on the context and on the moment. Adequate profiling is always dynamic and caught up in the loop of recognising a pattern (constructing the profile) and testing its salience (applying the profile).

Interestingly enough, such organic profiling is not dependent on conscious reflection. One could call it a cognitive capacity of all living organisms, without thereby claiming consciousness for an amoeba. One could also call it a form of intelligence based on the capacity to adapt: monitoring and testing, subsequent adaptation and repeated checking is what makes for the difference between the living and the inorganic world. This is what allows any organism to maintain its identity in the course of time, detecting opportunities to grow and spread as well as risks that need to be acted upon.

So, profiling is not typically human though we have developed our own brand of profiling, termed stereotyping by cognitive psychologists (Spears et al. 1997), and categorisation by Schauer (2003) in his *Profiles, Probabilities and Stereotypes*. What is special about humans is their capacity —according to brain scientists neatly embodied in the prefrontal cortex—to reflect upon the profiles they come up with. This is a rare capacity, closely related to consciousness and language, and we shall not explore this domain much further, leaving it at the nexus of neurosciences and philosophy of mind (Haggard and Libet 2001; Overgaard 2001). What matters is our capacity for conscious reflection on the profiles that we have unconsciously generated, because this gives us the freedom to deliberate on them, to reject or to reinforce them and deliberately to apply them. As Rouvroy (2008) saliently describes this is what allows our self-formation. It is the precondition for our actions to be qualified as stemming from the freedom to act: we can become aware of the patterns that regulate our actions and review them to change our habits. Though most of our interactions are automated, handled autonomically by the habits that are inscribed in our bodies and in our brains, we can bring them to mind and scrutinize their relevance, validity, fairness and justice. This is what turns us into autonomous agents, capable of making a conscious choice for a course of action, deciding by which law to live. Autonomous derives from the Greek, *auto nomos*: self and law. We can live by our own law, and are therefore be held accountable for our own actions (Hildebrandt 2008a).

What *is* new? profiling machines

Automated profiling is new in three ways. First, we are not talking about profiling by organisms but about profiling by machines (Elmer 2004). Basically these machines are software programs 'trained' to recover unexpected correlations in masses of data aggregated in large databases. Second, we are not talking about making queries in databases, summing up the attributes of predefined categories, but about discovering knowledge we did not know to be 'hidden' in the data (Zarsky 2002–2003; Custers 2004). Thirdly, we cannot reflect upon the way that profiling impacts our actions because we have no access to the way they are produced and used. This last difference suggests that profiling hampers our freedom to act autonomously, a point we will return to below.

Automated profiling can be described as the process of knowledge discovery in databases (KDD), of which data mining (DM, using mathematical techniques to detect relevant patterns) is a part (Fayyad et al. 1996). KDD is generally thought to consist of a number of steps:

1. Recording of data
2. Aggregation & tracking of data

3. Identification of patterns in data (DM)
4. Interpretation of the outcome
5. Monitoring data to check the outcome (testing)
6. Applying the profiles

Only the third step is what is called data mining in the sense of using mathematical algorithms to locate correlations, clusters, association rules and other patterns. An example of such profiling, using genetic algorithms, is driver fatigue detection by Jin et al. (2007). This type of profiling is also called behavioural biometric profiling (BBP) and uses a combination of pupil shape, eye movement frequency and yawn frequency to check tiredness of a driver. The data are mined by means of a feed-forward neural network and a back-propagation learning algorithm. To be fair we must note that BBP is still in an early stage of development, even though some results are highly interesting.[3] Both Zarsky (2002–2003) and Custers (2004) emphasize that the knowledge generated by profiling machines is new. Zarsky speaks of data mining as 'answering questions users did not know to ask' (Zarsky 2002–2003: 4). He especially focuses on the difference between classification based on predefined classes and data mining techniques, which provoke unexpected clusters. Custers (2004:56–58) argues that this type of knowledge is new in comparison with traditional social science, which starts with a hypothesis concerning a population that is tested by applying it to a sample. He points out that in the case of KDD the hypothesis emerges in the process of data mining and is tested on the population rather than a sample. He also indicates that when trivial information turns out to correlate with sensitive information, an insurance company or an employer may use the trivial information to exclude a person without this being evident as unfair discrimination (called *masking*). His last point is that the recording of data by means of ICT makes it nearly impossible to delete records, especially as they are often shared across contexts. KDD can thus trace and track correlations in an ever-growing mass of retained data and confront us with inferences drawn from past behaviour that would otherwise be lost to oblivion (Solove 2004; Warner 2005).

So, we have two differences with autonomic organic profiling: (1) the profiling is performed by machines and (2) the type of knowledge it generates differs from 'classical' empirical statistics. This raises several questions in relation to privacy and security, especially with regard to the effectiveness of data protection legislation. Before moving to discuss these anticipated threats I will first describe the Vision of Ambient Intelligence and the 'Internet of Things', to explain why autonomic machine profiling may have a major impact on our lives. This should reinforce the need to discuss potential new threats to privacy, security and other basic tenets of democracy and the rule of law.

[3] See e.g. BBP for aggression detection by means of monitoring of sound, at http://www.soundintel.com/index-en.html. For an overview Yannopoulos et al. 2008.

A vision of ambient intelligence and 'the internet of things'

Both the European Commission (ISTAG 2001) and, for instance, Philips (Aarts and Marzano 2003), have invested heavily in what is called the vision of Ambient Intelligence (AmI), vaguely defined by its 'key elements' (Aarts and Marzano 2003:14), being: (1) embeddedness, meaning that networked devices are integrated into the environment; (2) context-awareness, since these devices can recognize you and your situational context; (3) personalisation, as they can be tailored towards your needs; (4) adaptiveness, meaning that they may change the environment in response to your behaviours; and (5) anticipatory, since they should anticipate your preferences without your deliberate input, the environment will always be one step ahead of you.

Related aspects that are often mentioned in the context of AmI are its hidden complexity, the absence of keyboards or monitors, the fact that the environment itself becomes the interface and its capacity to perform real time monitoring and ubiquitous and proactive computing.

The enabling technologies of this smart environment are sensor technologies, RFID systems, nanotechnology and miniaturization. Together they create *The Internet of Things* (ITU 2005), which is supposed to turn the offline world online. The 'Internet of Things' consists of things that are tagged and permanently observed while communicating their data through the network that connects them. We must keep in mind, though, that most of these technologies only generate an enormous amount of data, which may not reveal any knowledge until profiling technologies are applied. We may conclude that profiling technologies are the crucial link between an *overdose of trivial data* about our movements, temperature, and interaction with other people or things and *applicable knowledge* about our habits, preferences and the state of the environment. Only after running data mining techniques through the interconnected databases can the things in our environment become smart things and start acting like agents in a multi-agent network (MAN). Profiling thus creates the added value in the mass of data, of which we don't yet know what is noise and what is information.

The vision of AmI depends on a seamless adjustment of the environment to our inferred habits and preferences. The idea is that we need *not* provide deliberate input, but are 'read' by the environment that monitors our behaviour. This presumes what Tennenhouse (2000) describes as proactive instead of interactive computing, diminishing human intervention as far as possible. To adapt the environment seamlessly we cannot afford to wait for a human interpreter but need profiling machines that draw their own conclusions about what we prefer when and where, hoping we can thus solve the problem of endless choice and deliberation.

Democracy and the rule of law

Before describing the threats afforded by the socio-technical infrastructure of AmI and the Internet of Things, we need to decide on what kind of threats we wish to detect. In this contribution the focus is not only on threats to individual consumers or taxpayers, but also on potential threats against the socio-legal and political

framework of democracy and the rule of law. This framework is a historical artefact, providing the constitutional instruments for individual citizens to counter threats to their rights and liberties. To make sense of potential threats against democracy and the rule of law, we will first discuss how these terms are to be understood in relation to profiling.

A sustainable democracy presumes and maintains the rule of law. The rule of law is often defined in reference to the protection of human rights and limited government. With regard to the implications of profiling technologies the most relevant achievement of the rule of law seems to be the mix of what Berlin (1969) has coined as negative and positive freedom (Hildebrandt 2008). Positive freedom—*freedom to*—regards the freedom to participate in public decision-making processes or the freedom to achieve one's personal objectives; negative freedom or liberty—*freedom from*—regards the absence of unreasonable constraints imposed on a person. Positive freedom has a long history, while negative freedom—as a value of liberal democracy—is a relatively recent invention. Felix Stalder (2002) in fact suggests that privacy, with its emphasis on negative freedom, is an affordance of the era or the printing press. To nourish a sustainable democracy we need both types of freedom, as embodied in the rule of law (Gutwirth and De Hert 2005). For this reason privacy is not just a private interest but also a public good. The rule of law establishes constitutional protection of citizens' rights and liberties over and against their government, safeguarded by an independent judiciary that shares the authority of the state. This is called the paradox of the Rechtsstaat: the state gives its authority to those that judge citizens who contest the way the state uses its authority in a given case.

Profiling can endanger both negative and positive freedom. Negative freedom is often equated with opacity, retreat to a private space-the right to oblivion and invisibility to the public eye. It refers to a space and time to regain one's strength, to reflect upon one's objectives and opinions. This negative freedom is matched with a need to act, to anticipate and participate in the public space, for which some measure of transparency is needed. Without transparency one cannot anticipate or take adequate action. In fact I would claim that negative freedom is an illusion as long as transparency is absent, as we may think that we are facing up to reality in the privacy of our own thoughts, while in fact we have no access to the knowledge needed to assess this reality. Thus profiling may endanger the intricate combination or negative and positive freedom whenever we (1) think we are alone, but are in fact watched by machines that observe our online behaviour, and in an AmI world any move we make; and (2) think we are making private decisions based on a fair idea of what is going on, while in fact we have no clue as to why service providers, insurance companies or government agencies are dealing with us the way they do.

Referring to what has been discussed in section 2 we should admit that most of our interactions take place without conscious reflection; they are a type of *autonomic* behaviour that is the result of individual learning processes that enable us to move smoothly through everyday life. This, in itself, is not a violation of our negative or positive freedom. As a result of learning processes it may even be the result of the way we exercised our freedom in the past (Varela 1992). However, *autonomous* action (other than autonomic behaviour) is related to the possibility of deliberate reflection on our choices of action. For this we need to have access to the knowledge

that impacts these choices. Targeted servicing, customisation and filtering of information could otherwise provide us with a comfortable, golden cage (Sunstein 2001); allowing us a reflexive life without reflection (Lessig 1999).

Threats: knowledge is power

The potential threats of profiling must not be conflated with those of data collection per se. First, the implications of profiling for the autonomy of individual citizens do not depend on the collection of personal data but on the processing and mining of these data. The resulting profiles, which are applied to a person because her data match the profile, are often generated by data mining other people's data. What should concern us here is the process of constructing profiles and their application to people whose data were not used to build the relevant profiles (disabling the applicability of the data protection directive that is focused on the protection of personal data).[4] Informational privacy is all too often reduced to a private interest in the hiding of personal data. This reductionism misses the *knowledge* asymmetry between profilers and profiled, which has far more implications than the information asymmetry that focuses on access to personal data. Second, because of the reduction of privacy to mere non-disclosure of personal data, privacy is often depicted as a private good, to be traded against other goods. However, in acknowledging that privacy is not only about personal data, we must face the fact that privacy is also a public good that concerns a citizen's freedom from unreasonable constraints on the construction of her identity (Agre and Rotenberg 2001; Hildebrandt 2006; Rouvroy 2008).[5] This freedom is a precondition for democracy and rule of law, as we have argued in the previous section. The hiding of personal data—which seems a Pavlovian reaction by lawyers and other privacy advocates—will, however, not protect us from the impact of group profiling on the construction of our identity, while at the same time hiding personal data will reduce the quality of the profiles (and the intelligence of the environment). Third, in the discourse on public and private security, we are often called upon to trade part of our privacy (understood as non-disclosure of personal data) for security. However, neither privacy nor security are fit for private trading. While privacy is a public good in as far as it is constitutive of human agency in a constitutional democracy, security one of the *raisons d'être* of the state. A state that does not provide its citizens with a minimum of security is qualified as what we call a failed state, incapable of protecting citizens against each other and against abusive state officials. As in relation to the so called trade-off between privacy and security two points can be made: (1) a loss of privacy may imply a loss of security, because it exposes the vulnerability of human identity,

[4] D 95/46/EC. The data protection directive aims to protect personal data, defined as 'any information related to an identified or identifiable person' (article2, sub a). See 'Opinion 4/2007 on the concept of personal data', of the Article 29 Working Party, WP136 2007. The question of what data qualify as personal data is controversial and may become thus contextual that legal certainty as to which data fall within the scope of the directive is lost.

[5] In speaking of the construction of one's identity we endorse a relational non-essentialist conception of identity. See Hildebrandt 2008a, at 312-315 and Hildebrandt et al. 2008 on human identity as the nexus of *idem* and *ipse*.

which renders even more complicated the idea of a trade-off between the two;[6] and (2) trading of personal data implies co-modification and with Schwartz (2000) we may expect a market failure due to the unequal access to information about the consequences of trading one's personal data (especially in the case of profiling).[7]

Profiling machines may spy on you, but why should you care about a machine watching your daily business? In AmI, most of the monitoring and adaptation will be a matter of machine-to-machine communication (M2M), while these machines will not be interested in who you are but in what profit can be gained from which category you fit. How does this relate to privacy and security as what Schwartz (2000) calls constitutive (public) values, aiming to provide citizens with a kind of agency that is presumed in constitutional democracy? As for profiling, privacy and security both seem to revolve around the question 'who is in control: citizens or profilers?' But again control is often reduced to hiding or disclosing personal data and this does not cover privacy and security as public values.

To come to terms with potential threats we need to look deeper into the asymmetries between citizens on the one hand and large organisations that have access to their profiles on the other hand. We are not referring to the asymmetry of effective access to *personal data* but to the asymmetry of effective access to *knowledge*. Especially in as far as this knowledge is protected as part of a trade secret or intellectual property the citizens to which this knowledge may be applied have no access whatsoever. Zarsky (2002–2003) has demonstrated—by analysing a set of examples—how this lack of access can lead to what he calls the 'autonomy trap'. Precisely because a person is not aware of the profiles that are applied to her, she may be seduced to act in ways she would not have chosen otherwise. Imagine that my online behaviour is profiled and matched with a group profile that predicts that the chance that I am a smoker who is on the verge of quitting is 67%. A second profile predicts that if I am offered free cigarettes together with my online groceries and receive news items about the reduction of dementia in the case of smoking I have an 80% chance of not quitting. This knowledge may have been generated by tobacco companies, which may use it to influence my behaviour. In a way, this kind of impact resembles Pavlov's stimulus-response training: it does not appeal to reason but aims to discipline or seduce me into profitable behaviour. My autonomy is circumvented as long as I am not aware of the knowledge that is used. Zarsky (2002–2003) also warns about unfair discrimination, based on refined profiling technologies that allow sophisticated market segmentation. Price discrimination may be a good thing in a free market economy, but the fairness again depends on the awareness of consumers of the way they are categorised (Odlyzo 2003). In order to have a fair and free market economy some rules of the game must be established to prevent unequal bargaining positions, or else we will produce another market failure.

[6] Schneier (2006) suggests that security always involves trade-offs and we had better get used to it. He argues that we should demystify security and start making sensible security trade-offs. My point is that even if both security and privacy involve trade-offs, we should get over the idea that trading privacy for security will indeed provide long term security. The interrelationship between the two is far too complex and we had better invest our energy in win-win solutions (cf. Cavoukian and Hamilton 2002).

[7] Schwartz (2000, at 745) refers to the Calabresis-Melamed analysis that states that property rules work well in the case of few parties, difficult valuations, low transaction costs, while liability rules work well in the case of many parties, monopoly, strategic bargaining and high transaction costs.

In short the threats can be summarised as concerning (1) privacy, which, however, must not be reduced to hiding one's personal data; (2) security, which, however cannot be traded with privacy since a loss of the one may cause the loss of the other); (3) unfair discrimination, meaning that power relations must be balanced to provide equal bargaining positions; and (4) autonomy, meaning that our negative and positive freedom to act must be established and maintained, since manipulation on the basis of knowledge that we are not aware of violates our autonomy.

Legal pitfalls and challenges

Data have a legal status. They are protected, at least personal data are. Europe tends to understand this protection as a personality right, which opens the possibility to declare certain data to be inalienable. In practice, however, the leaking of personal data is taken to imply consent for storing and using them. Whatever the written safeguards we find in the data protection directive, in practice most people most of the time do not even have an inkling of what is happening to which data resulting in the application of which profiles. Some American scholars, notably Lessig (1999), favour co-modification in order to facilitate trading one's personal data. In their eyes this should provide at least some kind of citizen's control. However, as discussed above with reference to Schwartz (2000), one may expect a market failure in the sense that due to grotesque knowledge asymmetries the implied consent will be based on ignorance—just like it is today. In both cases one of the problems is that we have no access to the group profiles that have been inferred from the mass of data that is being aggregated and have not the faintest idea how these profiles impact our chances in life. It may be time to reconsider the legal focus on the protection of personal data, as well as the focus of the privacy advocates who invest in privacy enhancing technologies. What we need is a complementary focus on the dynamically inferred group profiles that need not be derived from one's personal data at all, but may nevertheless contain knowledge about one's probable (un)healthy habits, earning capacity, risk-taking, life style preferences, spending habits, political associations etc.

Profiles have no clear legal status. That is, they may be *protected from* access via intellectual property rights by the profiler or be considered part of a company's trade secrets.[8] Protection against, or at least access to profiles is very limited. In data protection legislation one can locate two ways to claim access to a profile. First one can argue that once a profile has been applied to an individual person it becomes a personal data, e.g. in the case of credit scoring practices. This however, does not concern the relevant group profile or its relation to other group profiles, nor the way the profile was generated (by use of which algorithm etc.).[9] Second one can argue

[8] Cf. section 41 of the preamble of D 95/46 EC.

[9] The relevant group profile may determine the credit score, which is then a personal data. The profile would indicate that all people with a specific mix of attributes (concerning income, neighbourhood, credit history, gender, profession, educational background) entails a specific credit-risk. This group profile applies to a number of people, it is the result of data mining and not a personal data in the sense of the directive.

that autonomic application of profiles falls within the scope of article 15 of the Data Protection Directive (D 95/46 EC). Paragraph 1 of this article reads:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him.

In short, this article seems to grant European citizens a right not be subjected to an automated decision in the case that this decision makes a difference to their life. However, this safeguard has four pitfalls. First, like Bygrave (2001) suggests, it may be that if I don't exercise the right, the automated decision is not a violation of the directive. Second, the 2nd paragraph of article 15 reads:

> Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
>
> (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
>
> (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

This seems to create many loopholes for automated application of profiles. The third pitfall concerns the fact that as soon as the decision is not automated due to a (routine) human intervention the article no longer applies. In the case of autonomic profiling in an AmI environment this would not be an option, because the seamless real time adjustment of the environment rules out such human intervention. This brings us to the fourth and last pitfall: as long as one is not aware of being subject to such decisions one cannot exercise this right. The fact that article 12 grants the right to know 'the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in article 15 does not really help if one doesn't know about the automated decisions in the first place. This is the case even if after application the profile may in fact be a personal data and fall within the scope of articles 11 and 12, which obligate the relevant decision maker to notify the data subject and provide access to the data. In other words: today's technological and organisational infrastructure makes it next to impossible seriously to check whether and when the directive is violated, creating an illusion of adequate data protection. As Hosein (2005) has argued, the American approach may in fact deliver better results due to the constitutional protection that can be claimed and the more vigilant character of civil society in the US.

In seems that we have a double challenge here. First, the existing legal framework lacks adequate protection with regard to the application of group profiles. The right of access to the logic of processing is restricted to very specific circumstances that seldom apply. Apart from that, the fact that such profiles are generally protected by means of trade secret or intellectual property turns the legal right of access to the

logic of processing into an empty shell. Second, in as far as the directive does grant legal rights of access to relevant group profiles we need a technological and organisational infrastructure to enable the exercise of these rights. Without such a socio-technical infrastructure the directive does not gives us an effective remedy. This would entail real time information for individual citizens about profiles that may be applied to them, including the potential consequences. Only if such an infrastructure is in place can the rule of law, especially the particular mélange of positive and negative freedom discussed above, be sustained.

Transparency enhancing tools: from PETs to TETs

The idea that legal protection requires articulation into the technological infrastructure against which protection is warranted,[10] seems to gain currency. On 15th March 2007, after an extensive public consultation during 2006, the European Commission has presented its Communication on RFID.[11] The Commission starts out with claiming a beneficial social contribution of RFID in a number fields: safety (e.g., food traceability, anti-counterfeiting of drugs), convenience (e.g., shorter queues in supermarkets, more accurate and reliable handling of luggage at airports, automated payment), accessibility (e,g, patients suffering from dementia and Alzheimer's disease), healthcare (increased quality of case and safety), retail and industry (supply chain management), protection of the environment (e.g. recycling). Next to the social contribution the Commission expects RFID to boost industrial innovation and growth potential. After this, the issues of data protection, privacy and security are dealt with in reference to the Data Protection Directive and the ePrivacy Directive.[12] Regarding the Data Protection Directive the Commission notes that the Member States will have to ensure that the introduction of RFID applications complies with privacy and data protection legislation, necessitating the drawing up of specific codes of conduct. The Commission indicates that the national data protection authority and the European 'Article 29 Working Party'[13] will have to review these codes of conduct and monitor their application.

What about the fact that the national data protection authority lacks the resources seriously to monitor what is happening? We only need to refer to the transfer of transaction data of European banks and Swift to the US Department of Treasury (UST) authorities to realise that organisations do not feel compelled to notify citizens of the way their data are used, unless forced to by widespread publicity (ICPP 2006; Boon 2007).[14] The Commission is of the opinion that the response to the challenges

[10] Modern law is articulated in the technology of the script and can seen as an 'affordance' of the printing press. About the idea that legal norms need articulation in the digital infrastructure that is emerging today, see M. Hildebrandt (2008b). Also M. Hildebrandt and B.J. Koops (2007).

[11] COM(2007)96 final.

[12] D 2002/58/EC.

[13] See Article 29 Working Party WP105, 2006.

[14] See Article 29 Working Party WP128, 2006.

posed by RFID technologies should include the 'adoption of design criteria that avoid risks to privacy and security, not only at the technological but also at the organisational and business process levels'.[15] This is an interesting option. It refers to what has been called constructive technology assessment (CTA), initiated by e.g. Rip et al. (1995), building a case for 'upstream' involvement in technological design, i.e. not installing ethical commissions after the technology is a finished product but getting involved at the earliest possible stage of technological design. As we may guess designers' good intentions do not determine the actual affordances of a technology, due to the multi-stability of technological artefacts (Ihde 1990). This means that one and the same technology often affords different behaviours, while it is not always easy to anticipate which behaviour will emerge once the technology is integrated in the socio-technical context of its users. Multi-stability, however, does not mean that anything goes, or that it makes no sense to anticipate the affordances of technologies under construction. On the contrary, multi-stability means that upstream involvement of potential end-users and others who may be affected by the technologies, will broaden the scope of technical design and increase the opportunities to construct a socio-technical infrastructure that does not obstruct the flourishing and autonomy of individual citizens.

RFID-based systems are one of the enabling technologies of 'The Internet of Things' and AmI (Hildebrandt and Meints 2006). They produce an immense amount of data about (change of) location and if linked to other data they provide a rich resource for profiling practices. Which technological and organisational infrastructure will provide the transparency of profiles that we argued above? The Commission mentions its support for privacy-enhancing technologies (PETs), 'to mitigate privacy risks'.[16] However, as stated above PETs focus on the hiding of data (anonymisation) and on the use of pseudonyms, which may provide a kind of what Nissenbaum (2004) has coined contextual integrity. Countering the threats of autonomic profiling citizens will need more than the possibility of opting out, it will need effective transparency enhancing tools (TETs) that render accessible and assessable the profiles that may affect their lives.[17]

For this reason we end this contribution with an appeal to rethink the legal-technological infrastructure in order to give profiles an effective legal status. This should provide citizens, whether as consumers, patients or targets of government investigations, with the legal and technological tools to understand which profiles may impact their life in which practical ways. Rethinking the legal-technological infrastructure is a major challenge. Evidently, commercial enterprise has an interest in protecting its trade secrets or its intellectual property rights in databases or software programmes. The tension between rights of access and corporate property rights has been acknowledged in section 41 of the preamble of the Data Protection

[15] COM(2007)96 final, at 6.

[16] COM(2007)96 final, at 11.

[17] Cp. Gutwirth and De Hert (2005) about the fact that data protection legislation is mainly a transparency tool, while privacy is considered to be an opacity tool. My point is that the transparency aimed for by the present generation of data protection regimes concerns personal data, without taking note of the results of data processing. The results, consisting of highly sophisticated group profiles, urgently need effective transparency tools.

Directive, but no serious effort has been made to investigate further how this tension can be resolved or made productive in a way that safeguards human self-determination. It may be, however, that even if legal and technological transparency tools are developed, we are faced with more demanding challenges. These concern the complexity of the profiling processes and the growth of information they engender (Kallinikos 2006). First, the complexity as well as the quantity of information produced by transparency enhancing technologies could overwhelm an individual person, if this information were provided in the form of text, requiring conscious reflection. TETs will only succeed in empowering citizens if the human-machine interfaces (HMIs) that mediate between the environment and the individual are as seamless and ubiquitous as the AmI infrastructure they aim to render transparent. TETs should allow a person to play around with the environment in order to guess how her behaviours trigger proactive interventions of the environment (Nguyen and Mynatt 2002); they should not flood a person with detailed technical information that requires her attention in a way that nullifies all the 'advantages' of ubiquitous and seamless computing. The HMIs will have to communicate the relevant information in a way that allows one to have 'a feel' of the environment's interpretation of one's behaviour, rather than text. This, however, does not mean that a more precise access to the technical details must not be available, for instance to enable one to contest the application of profiles in a court of law. This brings us to a second major challenge, which concerns the fact that at some point such technical detail cannot be provided, owing to the fact that autonomic profiling will be self-repairing, self-healing and self-managing to an extent that turns the whole process into a black box that even the designer of the process cannot open. And, to further complicate the issue, even if the technical detail could be disclosed, the human mind could not possibly follow—let alone explain—what happens inside the profiling machines. To follow and check this we would need another machine with similar or even more computing capacities (Van Bendegem 2008). These challenges should not paralyse us. They should, instead, be a wake-up call for lawyers, politicians and computer engineers to join forces during the construction of the smart infrastructures in which so much capital is presently being invested. These new digital infrastructures will match the printing press in terms of their impact on the structure of our societies and this warrants speculative even if rigorous investigation as well as sustained interdisciplinary dialogue.

Closing remarks

Advanced profiling technologies answer questions we did not raise. They generate knowledge we did not anticipate, but are eager to apply. As knowledge is power, profiling changes the power relationships between the profilers and the profiled. These asymmetries challenge the relative autonomy of individual citizens and allow an unprecedented dynamic segmentation of society, especially if the vision of Ambient Intelligence is realised: based on refined real time monitoring, followed by proactive adaptation of our smart environment. As long as we lack the legal and technological infrastructure to counter the emerging asymmetry we may find ourselves in a gilded cage: an environment that anticipates our preferences before we

become aware of them. This contribution argues that we urgently need to develop legal and technological transparency enhancing tools (TETs) to match the proactive dimension of our smart environments. This will require substantial cooperation between social scientists, computer engineers, lawyers and policy makers with a clear understanding of what is at stake in terms of democracy and the rule of law. Such cooperation will allow us to sustain the legal-political framework that safeguards the right to be free from unreasonable constraints on the construction of identity in information society.

References

Aarts E, Marzano S (eds.). The New Everyday. Views on Ambient Intelligence. 010: Rotterdam; 2003.

Agre PE, Rotenberg M (eds.). Technology and Privacy: The New Landscape. MIT Press: Cambridge, Massachusetts; 2001.

Article 29 Working Party. Working paper 105 on data protection issues related to the RFID technology. Brussels; 2006, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

Article 29 Working Party. Working paper 128 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Brussels; 2006, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

Article 29 Working Party. Working paper 136, Opinion 4/2007 on the concept of personal data. Brussels; 2007, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

Berlin I. Two concepts of liberty. Idem. Four essays on liberty. Oxford University Press: Oxford New York; 1969. p. 118–173.

Boon v d, Vasco. Banken melden klant dat VS gegevens inzien. Informatiecampagne om privacyproblemen te verhelpen. Het Financieel Dagblad; 2007, p. 1.

Bygrave,L. Minding the Machine. Article15 and the EC Data Protection Directive and automated profiling, 17 Computer Law & Security Report, 2001-1**:** 17–24

Cavoukian A, Hamilton T. The Privacy Payoff. How Successful Businesses Build Consumer Trust. McGraw-Hill Ryerson Limited: Toronto; 2002.

COM(2007)96 final. Communication on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. European Commission: Brussel; 2007.

Custers B. The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Wolf Legal Publishers: Nijmegen; 2004.

Elmer G. Profiling Machines. Mapping the Personal Information Economy. MIT Press: Cambridge, Mass; 2004.

Fayyad UM, Piatetsky-Shapiro G, Smyth P, Uthurusamy R. Advances in Knowledge Discovery and Data Mining. AAAI Press / MIT Press Meno Park: California - Cambridge, Mass. - London England; 1996.

Gutwirth S, De Hert P. Privacy and Data Protection in a Democratic Constitutional State. In: Hildebrandt M, Gutwirth S (eds.). Profiling: Implications for Democracy and Rule of Law, FIDIS deliverable 7.4. Brussels; 2005, available at www.fidis.net.

Haggard P, Libet B. Conscious intention and brain activity. J Conscious Stud. 2001;8(11):47–63.

Hildebrandt M. Privacy and Identity. In: Claes E, Duff A, Gutwirth S (eds.). Privacy and the Criminal Law. Intersentia: Antwerp; 2006. p. 43–58.

Hildebrandt M. 'Defining Profiling: A New Type of Knowledge and Profiling' and 'The Identity of the European Citizen'. In: Hildebrandt M, Gutwirth S (eds.). Profiling the European Citizen. A Cross-disciplinary Perspective. Springer: Dordrecht; 2008a. p. 17–30 and 303–26.

Hildebrandt M. A Vision of Ambient Law. In: Roger B, Yeung K (eds.). Regulating technologies, Hart: Oxford; 2008b.

Hildebrandt M, Meints M. (eds.). RFID, Profiling and Ambient Intelligence. FIDIS deliverable 7.7: Brussls; 2006, available at www.fidis.net.

Hildebrandt M, Koops BJ (eds.). A Vision of Ambient Law. FIDIS deliverable 7.9; 2007, available via www.fidis.net.

Hildebrandt M, Koops BJ, de Vries K (eds.). Where Idem-Identity meets Ipse-Identity. Conceptual Explorations. FIDIS deliverable 7.14, Brussels; 2008, forthcoming, will be available at www.fidis.net.

Hosein G. Threatening the Open Society: Comparing Anti-Terror Policies in the US and Europe. Privacy International: London; 2005.
ICPP. Opinion delivered by the Independent Centre for Privacy Protection at the Federal State of Schleswig-Holstein (ICPP) on the International bank data transfer by Schleswig-Holstein financial institutions using Swift; 2006. Available at: https://www.datenschutzzentrum.de/index.htm.
Ihde D. Technology and the Lifeworld. From Garden to Earth. Indiana University Press: Bloomington and Indianapolis; 1990.
ISTAG. Scenarios for Ambient Intelligence in 2010. Information Society Technology Advisory Group; 2001**:** available at: http://www.cordis.lu/ist/istag-reports.htm.
ITU. The Internet of Things. International Telecommunications Union (ITU), Geneva; 2005
Jin S, Park S-Y, Lee JJ. Driver Fatigue Detection Using a Genetic Algorithm. Artificial Life and Robotics 11; 2007 (1): 87–90.
Kallinikos J. The Consequences of Information. Institutional Implications of Technological Change. Edward Elgar, Cheltenham, UK Northampton: MA, USA; 2006.
Lessig L. Code and other laws of cyberspace. Basic Books: New York; 1999.
Maturana HR, Varela FJ. Autopoiesis and Cognition: The Realization of the Living. Reidel: Dordrecht; 1991.
Nissenbaum H. Privacy as Contextual Integrity. 79 Washington Law Review 2004-1; 101–140.
Nguyen D, Mynatt E. Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems, Technical Report GIT-GVU-02-16. Georgia Institute of Technology: USA; 2002.
Odlyzko AM. Privacy, economics, and price discrimination on the Internet. In: Sadeh N editor. ICEC2003: Fifth International Conference on Electronic Commerce, ACM; 2003, pp. 355–366.
Overgaard M. The Role of Phenomenological Reports in Experiments on Consciousness. 12 Psycoloquy; 2001-29.
Rip A, Misa TJ, Schot J. Managing Technology in Society: The Approach of Constructive Technology Assessment. Pinter Publishers: London; 1995.
Rouvroy A. Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. 2 Studies in Ethics, Law, and Technology; 2008-1, Article 3, available at: http://www.bepress.com/selt/vol2/iss1/art3.
Schauer F. Profiles Probabilities and Stereotypes. Belknap Press of Harvard University Press: Cambridge, Massachusetts / London, England; 2003.
Schneier B. Beyond Fear. Thinking Sensibly About Security in an Uncertain World. Copernicus Books: New York; 2006.
Schwartz PM. Beyond Lessig's *Code* for Internet Privacy: Cyberspace Filters, Privacy-Control and Fair Information Practices. Wisconsin Law Review; 2000, p. 743–788.
Scott JC. Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed. Yale University Press: New Haven and London; 1998.
Spears R, Oakes PJ, Ellemers N, Haslam SA. (eds.). The Social Psychology of Stereotyping and Group Life. Blackwell: Oxford; 1997.
Solove DJ. The Digital Person. Technology And Privacy In The Information Age. New York University Press: New York; 2004.
Stalder F. The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy, 7 Sociological Research Online, 2002- 2, available at <http://www.socresonline.org.uk/7/2/stalder.html>.
Sunstein C. Republic.com. Princeton University Press: Princeton and Oxford; 2001.
Tennenhouse D. Proactive Computing. 43 Communications of the ACM 2000-5, p. 43–50.
Torpey J. The Invention of the Passport. Surveillance, Citizenship and the State. Cambridge University Press: Cambridge; 2000.
Van Bendegem JP. Neat Algorithms in Messy Environments. In: Hildebrandt M, Gutwirth S (eds.). Profiling the European Citizen, Cross-Disciplinary Perspectives. Springer: Dordrecht; 2008. p. 80–83.
Varela FJ. Ethical Know-how. Stanford University Press: Stanford; 1992.
Warner J The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps, 2 university of ottawa law & technology journal; 2005-1, p. 75–105
Yannopoulos A, Androniki V, Varvarigou T. Behavioural Biometric Profiling and Ambient Intelligence. In Hildebrandt M, Gutwirth S (eds.). Profiling the European Citizen. Cross-Disciplinary Perspectives, Springer: Dordrecht 2008, p. 89–104.
Zarsky T Z. "Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion, 5 Yale Journal of Law & Technology 2002–2003, nr. 4**,** p.17–47.