May, 2010

The Challenges of Ambient Law and Legal Protection in the Profiling Era

Mireille Hildebrandt
Bert-Jaap Koops

THE MODERN LAW REVIEW

The Challenges of Ambient Law and Legal Protection in the Profiling Era

Mireille Hildebrandt and Bert-Jaap Koops*

Ambient Intelligence is a vision of a future in which autonomic smart environments take an unprecedented number of decisions both for the private and the public good. It involves a shift to automated pattern recognition, a new paradigm in the construction of knowledge. This will fundamentally affect our lives, increasing specific types of errors, loss of autonomy and privacy, unfair discrimination and stigmatisation, and an absence of due process. Current law's articulation in the technology of the printed script is inadequate in the face of the new type of knowledge generation. A possible solution is to articulate legal protections within the socio-technical infrastructure. In particular, both privacy-enhancing and transparency-enhancing technologies must be developed that embed legal rules in ambient technologies themselves. This vision of 'Ambient Law' requires a novel approach to law making which addresses the challenges of technology, legitimacy, and political-legal theory. Only a constructive and collaborative effort to migrate law from books to other technologies can ensure that Ambient Law becomes reality, safeguarding the fundamental values underlying privacy, identity, and democracy in tomorrow's ambient intelligent world.

INTRODUCTION

Ambient Intelligence is a vision of a future world in which autonomic smart environments take an unprecedented number of decisions for us and about us, in order to cater to our inferred preferences. In such a world, waking up will be accompanied by a personalised influx of light and music; coffee will be ready at the right moment and with the correct measures of sugar, milk, and caffeine in accordance with personal taste and budget; food will be ordered in tune with one's lifestyle – possibly including health-related restrictions; the drive to the office will be organised by one's smart car that communicates with other cars and traffic monitoring systems; office buildings will be accessible for those chipped with the right ID; incoming messages will be sorted in terms of urgency and importance; and agendas will be reconfigured in light of automatically inferred work-flow requirements.

Ambient Intelligence builds on profiling techniques or automated pattern recognition, which constitutes a new paradigm in the construction of knowledge.

*Mireille Hildebrandt is Associate Professor of Jurisprudence at the Erasmus School of Law, Rotterdam and Senior Researcher at the Vrije Universiteit Brussel. Bert-Jaap Koops is Professor of Regulation & Technology at Tilburg University, the Netherlands. This article was written as part of the EU-funded project FIDIS (Future of Identity in the Information Society, see http://www.fidis.net). It is also based on the findings of the first author's research in the GOA project on 'Law and autonomic computing: mutual transformations', financed by the Vrije Universiteit Brussel, and on the results of the second author's Dutch NWO-funded VIDI project on law, technology and shifting balances of power. The authors thank Jozef Vyskoc, Els Soenens and two anonymous reviewers for their salient comments, and Morag Goodwin for her valuable help in editing.

Published by Blackwell Publishing, 9600 Garsington Road, Oxford OX4 2DQ, UK and 350 Main Street, Malden, MA 02148, USA

We will argue that this new paradigm will fundamentally affect our lives, and that the emerging socio-technical infrastructure generates several types of vulnerabilities. This raises the question of whether current law is sufficiently equipped to address these vulnerabilities. We will also argue that the characteristics of Ambient Intelligence call for a systematically different approach to legal protection if we are to safeguard citizens in the profiling era in light of these emerging vulnerabilities. We contend that the vision of Ambient Intelligence calls for a vision of an Ambient Law that inscribes legal protection into the socio-technical infrastructure, providing protection to the users, even if this poses novel challenges for legislators, policy-makers, businesses, and engineers.

To demonstrate why and how an Ambient Law should be developed, we have divided this paper into three parts. The first part considers the implications of Ambient Intelligence infrastructure for privacy, identity, and the rule of law. The answer focuses on the type of errors that can be expected, on the loss of autonomy and privacy, on unfair discrimination and stigmatisation, and on the absence of due process. The second part investigates the extent to which current law is able to address these vulnerabilities and how this relates to the current form of law. Building on previous work in which we explored the idea that in the face of Ambient Intelligence the articulation of law in the technologies of the script is inadequate, the present article concludes that the failure of current law is systemic. A possible solution to address the systemic gaps in legal protection is to articulate legal protections into the socio-technical infrastructure itself as it is under construction. Acknowledging the embodied character of the law, being a normativity that is currently articulated in technologies of the script (manuscripts and printing press), we argue that to prevent the rule of law from becoming obsolete as it is replaced by what will effectively turn out a mere rule of technology, legal protections will need to be articulated in the novel communication infrastructure itself. Several legal scholars have suggested similar undertakings, building on Lessig's idea of 'code as law' and Flanagan and Nissenbaum's 'values in design'. We have introduced the notion of Ambient Law to refer to such novel articulations. This leads to the third part of the paper which considers the ways in which the law should be changed in order to make the vision of Ambient Intelligence a reality at the same time as a vision of Ambient Law that embeds fundamental values in the ambient profiling technologies. This issue is taken up as a combination of technical, legal, and democratic challenges. It entails a smart kind of informational privacy that goes beyond an indiscriminate hiding of personal data. The point is to facilitate individual citizens' choice as to which of their data they want to hide, based on a measure of transparency of the profiles that match their personal data. This transparency – as well as the smart opacity it enables – requires the development of so-called transparency-enhancing as well as privacy-enhancing tools. As Ambient Law concerns the inscription of legal norms into the technical infrastructure, these tools are simultaneously legal and technological, raising the issue of how to prevent a 'rule of technology' while preserving the rule of law. We conclude that although the technical, legal, and democratic challenges can be analytically distinguished, they are entangled in practice. To establish such an Ambient Law, we therefore require novel approaches and a novel digital literacy to sustain the historical artefact of constitutional democracy.

PROFILING AND AMBIENT INTELLIGENCE

Ambient Intelligence

Ambient Intelligence refers to a research program, to a vision of the future, and to a novel paradigm.[1] The concept was introduced at the end of the 1990s by Philips and embraced by the European Commission as a vision of our technological future. Ambient Intelligence builds on earlier ideas about ubiquitous computing,[2] and envisions a further increase of computing systems that run our environment for us while their technological complexity is hidden behind the surface of things. In 1991, Mark Weiser launched the idea of ubiquitous computing:

> Inspired by the social scientists, philosophers, and anthropologists at PARC, we have been trying to take a radical look at what computing and networking ought to be like. We believe that people live through their practices and tacit knowledge so that the most powerful things are those that are effectively invisible in use . . . This is a challenge that affects all of computer science. Our preliminary approach: Activate the world. Provide hundreds of wireless computing devices per person per office, of all scales (from 1″ displays to wall sized). This has required new work in operating systems, user interfaces, networks, wireless, displays, and many other areas. We call our work 'ubiquitous computing'. This is different from PDA's, dynabooks, or information at your fingertips. It is invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere.[3]

Similarly, the vision of Ambient Intelligence assumes that keyboards and even computer screens will disappear as human-machine-interfaces. Instead, the environment will infer a person's preferences from her machine-readable behaviours, recorded by a set of invisible technologies, stored in large databases and mined by means of mathematical techniques that allow the detection of relevant patterns. The environment itself becomes the interface, infused with sensor technologies, radio frequency identification (RFID) systems, and behavioural and physical biometric profiling, all interconnected via online databases that store and aggregate the data that are ubiquitously captured.

Ambient Intelligence presents an adaptive environment that 'learns' what time you get up, how you like your coffee, which types of groceries you buy in the course of the week, what kind of news, mail, or calls are relevant for your professional life; it calculates what is important and what is urgent, in order to filter, sort, and prioritise incoming communications for you. Ambient Intelligence is

1 See E. Aarts and S. Marzano (eds), *The New Everyday: Views on Ambient Intelligence* (Rotterdam: 010 Publishers, 2003) and Information Society Technology Advisory Group, *Scenarios for Ambient Intelligence in 2010* (ISTAG, 2001) available at http://www.cordis.lu/ist/istag-reports.htm (last visited 28 December 2009); A. Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (Berkeley: New Riders, 2006); B. Van den Berg, *The Situated Self: Identity in a World of Ambient Intelligence* (Rotterdam: Erasmus Universiteit, 2009).

2 See his seminal text, M. Weiser, 'The Computer for the 21st Century' (1991) *Scientific American* 94. Weiser describes ubiquitous computing as the opposite of virtual worlds; instead of focusing on the realm of online interactions, ubiquitous computing involves the further computerisation of the offline world.

3 See http://www.ubiq.com/hypertext/weiser/UbiHome.html (last visited 28 December 2009).

based on proactive computing meant to adapt your environment to your preferences before you become aware of them. It organises your life at a subliminal level by seamlessly catering to your needs and desires and thus providing you with personalised opportunities based on a calculated anticipation of what you would have preferred had you known what the smart environment 'knows'. The environment becomes your 'digital butler', removing trivial worries, acting on your behalf – always based on stochastic inferences from your past behaviour, even calculating a measure of random diversion if that will make you feel better or more human (the machines may guess that we do not like to be entirely predictable).

Ambient Intelligence remains a future project. It could be rejected as an overly utopian – or dystopian – dream of technical engineers (and policy makers) who have lost touch with the real world. However, 'smart' applications are already in production and the pattern recognition methods they incorporate are creating a new type of knowledge-claim. According to some authors, the shift to automated pattern recognition involves the transition to a new paradigm in the construction of knowledge. In that light, the vision of Ambient Intelligence is to be taken seriously. Before moving into the implications for some of the basic assumptions of democracy and the rule of law, we will therefore first investigate the key enabling technology of 'smart' environments: autonomic pattern recognition, or profiling.

Profiling

As Schauer argues, profiling is an economical way of anticipating how a person's environment will behave in the near future.[4] It allows for a measure of generalisation that, while not always correct, will save time, energy, and attention, all scarce resources. The type of profiling that is a prerequisite for Ambient Intelligence is autonomic profiling,[5] based on pattern recognition in large databases. Profiling is defined here both as the construction or inference of patterns by means of data mining and as the application of the ensuing profiles to people whose data match with them. The application of profiles to new data allows recurrent testing of the profiles and further refinement. The construction of profiles is usually described as the process of 'knowledge discovery in databases' (KDD), which consists of three consecutive steps.[6] First, data are captured, stored, and aggregated. This involves a translation of real-life events to machine-readable data, while the aggregation involves choices that further format the resources for the next step. The second step, data mining, consists of applying algorithms to the data, aiming to discover patterns (clusters, association rules, correlations, etc) in

4 F. Schauer, *Profiles Probabilities, and Stereotypes* (Cambridge, Mass: Harvard UP, 2003).

5 J. O. Kephart and D. M. Chess, 'The Vision of Autonomic Computing' (2003) 36 *Computer* 41. The idea of autonomic computing is that just as our autonomic nervous system adapts our internal environment to sensory input, autonomic computing will adapt our external environment to data input.

6 U. M. Fayyad, G. Piatetsky-Shapiro *et al* (eds), *Advances in Knowledge Discovery and Data Mining* (Menlo Park, CA; Cambridge, Mass: MIT Press, 1996); T. Zarsky '"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion' (2002–03) 5 *Yale Journal of Law & Technology* 17.

the data that are not visible with the naked human eye. An algorithm can be used to test or verify whether a particular correlation between types of data can be confirmed; this is called top-down data mining or supervised learning. More interesting, however, is the use of bottom-up algorithms or unsupervised learning, which amounts to the detection of unexpected, novel patterns. This concerns a type of 'knowledge' that cannot be calculated by the human mind because of its limited 'working memory' and limited 'computing powers'.[7] Custers has indicated that this type of knowledge production is new and differs from traditional scientific methodology; instead of starting with a hypothesis and subsequently testing it in laboratory conditions, bottom-up data mining generates hypotheses that can be tested against new data that allow their real-time refinement.[8] The hypotheses that are generated and tested are correlations — not to be confused with causes or reasons — and some scientists provocatively claim that the age of data mining will have no more need for causal explanations:

> Scientists are trained to recognise that correlation is not causation, that no conclusions should be drawn simply on the basis of correlation between X and Y (it could just be a coincidence). Instead, you must understand the underlying mechanisms that connect the two. Once you have a model, you can connect the data sets with confidence. Data without a model is just noise.
>
> But faced with massive data, this approach to science — hypothesise, model, test — is becoming obsolete . . . There is now a better way. Petabytes allow us to say: 'Correlation is enough'. We can stop looking for models. We can analyze the data without hypotheses about what it might show. We can throw the numbers into the biggest computing clusters the world has ever seen and let statistical algorithms find patterns where science cannot.[9]

What should interest us here are the implications of actually using profiling technologies to invisibly categorise people, providing them with certain opportunities and attributing to them certain risks on the basis of their calculated inclinations and preferences. Ambient Intelligence is the most extensive vision of a world in which autonomic smart environments would take an unprecedented number of decisions for us and about us that would affect our chances in life. Though it is as yet unclear to what extent the investments made will in fact deliver a fully adaptive proactive environment, we think that it makes sense to anticipate at an early stage how the paradigm shift it incorporates will affect core legal principles like privacy, autonomy, equal treatment, fairness, and due process; once the socio-

7 This refers to the 'bounded rationality' of human cognition, a term coined in behavioural economics by Kahneman and Taversky, cf D. Kahneman, *Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice*, Prize Lecture Nobel Laureate, 8 December 2002, Nobel Prize in Economics documents 2004-2, 449–489 at http://nobelprize.org/nobel_prizes/economics/laureates/2002/kahnemann-lecture.pdf (last visited 28 December 2009). Bounded rationality may in fact be an advantage, most of the time, see G. Gigerenzer, *Gut Feelings: The Intelligence of the Unconscious* (New York: Penguin, 2007).

8 B. Custers, *The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology* (Nijmegen: Wolf, 2004).

9 C. Anderson, 'The End of Theory: The Data Deluge Makes the Scientific Method Obsolete' (2008) 16 *Wired Magazine* 7.

technical infrastructure that affords these smart environments is in place, it may be hard to redress some of its drawbacks.

Our vision of Ambient Law assumes that using written laws to regulate a world that has moved from the infrastructure of the script and the printing press to one of real-time wireless interconnectivity might well prove to be backing the wrong horse,[10] as written laws by themselves seem incapable of providing citizens with effective remedies in the era of smart computing.

VULNERABILITIES

Ambient Intelligence will undoubtedly bring opportunities to citizens in terms of convenience, living standards, safety, and the excitement factor of new technology. However, the scale and scope of ubiquitous profiling technologies will both create new vulnerabilities and aggravate existing ones. We distinguish four types of vulnerabilities: incorrect categorisation, privacy and autonomy, discrimination and stigmatisation, and the lack of due process. Though an extensive literature is available on the threat to privacy and of social sorting,[11] the first is often narrowly understood in terms of control over personal data and the second is often considered without taking into account the intricacies of KDD (as described above). We contend that another level of analysis, focused on the type of knowledge construction that is at stake, is warranted here in order to assess the implications of smart proactive technologies on the process of identity construction. It is precisely this process that is affected and that requires a thoughtful reflection on the extent to which profiling technologies threaten to subvert basic assumptions of democracy and the rule of law. Our investigation primarily concerns the normal usage of smart infrastructures, rather than their misuse or abuse, for example through identity theft, which merits separate treatment.[12] What we wish to highlight is that a novel communication and information framework implies a radically different context for a legal tradition that depends on the written and printed script for its legitimacy and effectiveness.

Errors

The first implication of the use of profiling technologies – distinct from their abuse or misuse – is that of the application of incorrect profiles due to 'errors' inherent in computing techniques based upon stochastic inferences. Profiling is based on statistical techniques and is thus vulnerable to the problem of false posi-

10 On the shift from written law to digital and Ambient Law, see M. Hildebrandt, 'A Vision of Ambient Law' in R. Brownsword and K. Yeung (eds), *Regulating Technologies* (Oxford: Hart, 2008).

11 D. Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (London: Routledge 2003).

12 See N. van der Meulen and B. J. Koops, 'The Challenge of Identity Theft in Multi-Level Governance. Towards a co-ordinated action plan for protecting and empowering victims' in J. van Dijk and R. Letschert (eds), *Globalisation, Victims, and Empowerment* (Springer, forthcoming) at http://ssrn.com/abstract=1447324 (last visited 28 December 2009).

tives and false negatives. Insofar as categorisation has an influence on a person's access to (virtual) spaces, services, or information, or on the price she has to pay for such access, profiling may be unfair if it treats a person as part of a category to which she does not in fact belong (false positive), or, vice versa, treats her as a person who does not belong to a category to which she in fact does (false negative). Being placed in a certain category is important not only for access to consumer goods and services but can have much more far-reaching consequences, for example concerning security issues or the likelihood of recidivism when being sentenced.[13]

In the case of autonomic profiling by a computerised, wirelessly interconnected smart environment, it is important to have an adequate understanding of the kind of profiles that are generated. Most of the profiling will not concern the data of one particular person, but rather the aggregated data of a mass of people. The patterns found in these data are group profiles that present a stochastic relation between a type of person and a type of behaviour or capacity. If the group profile is distributive, this means that the characteristics of the profiles apply equally to all members of the group. The group profile of a bachelor applies to all unmarried men. However, most group profiles are less tautological and non-distributive, meaning that even though the average or mean of the group correlates with certain characteristics, this does not apply to all members. For instance, a group profile that correlates certain behaviour to the onset of Parkinson's disease is distributive if every member of the group has a 67 per cent chance of developing Parkinson's disease; it is non-distributive if – on average – the members have a 67 per cent chance of developing the disease. In the latter case, a particular person could in fact have only a five per cent chance, due to other factors that correlate negatively with Parkinson's; but because group profiles 'abstract' from these other factors, this particular person may be treated as if her chance is 67 per cent, with all the attendant consequences for how she and others calculate her risk profile.[14] Thus, where a group profile is non-distributive, and data mining mainly generates non-distributive group profiles, autonomic profiling creates errors that are likely to lead to unjustified discrimination, based on incorrect assumptions.

A second problem that may arise concerns a sophisticated version of the Thomas theorem. Inferring preferences on the basis of past behaviour entails that people will be categorised and treated in line with their inferred group-profile, which may result in 'normalising' them into the kind of behaviour the profile predicts.[15] As Thomas and Thomas suggested, 'if men define situations as real, they will be real in their consequences'.[16] However, with machine profiling we face socio-technical infrastructures – instead of men — that 'define' situations as real, poten-

13 On the problems of profiling in policing and sentencing, see B. E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (Chicago: University of Chicago Press, 2006).

14 On non-distributive group profiles, see A. Vedder, 'KDD: The challenge to individualism' (1999) 1 *Ethics and Information Technology* 275.

15 Custers, n 8 above, 76–77. L. Lessig, *Code and other laws of cyberspace* (New York: Basic Books, 1999) 154. It is interesting to note a similarity with the Foucauldian notion of normalisation (associated with the advent of the statistical sciences).

16 W. I. Thomas and D. S. Thomas, *The Child in America: Behavior Problems and Programs* (New York: Knopf, 1928) 571–572.

tially producing the kind of behaviour they have inferred on the basis of group profiles.

This raises the question of whether machine-profiling is merely an extension of the normalisation practices already described by Foucault, Thomas, and Merton (bien étonnés de se trouver ensemble),[17] or whether the fact that these practices rely on machines constitutes a relevant difference. To the extent that an Ambient Intelligent environment tempts people to behave in the way the environment expects them to behave, the question of human autonomy is raised next to that of unjustified discrimination (which is based on incorrect assumptions).

If we assume that the errors we face here are not the result of abuse or misuse, but based on the fact that smart technologies depend on the 'mining' of aggregated machine-readable data, a number of epistemological issues surface. Prominent amongst these is the question of what it means to be anticipated by machines that produce knowledge by means of the manipulation of discrete machine-readable data. We will discuss this under the heading of privacy, social sorting and due process.

Loss of autonomy and privacy

By providing an adaptive environment that does not bother the user with requests for deliberate input, Ambient Intelligence communicates on a subliminal level. In doing so, it deprives users not only of the means to reflect on the choices their environment makes for them, but may proactively impact the choices that users make. For example, if I am contemplating becoming vegetarian, profiling software may infer this from my online behaviour. It may for instance infer that there is an 83 per cent chance that I will stop eating meat within the coming month and sell this information to a retailer or industry that has an interest in me remaining a carnivore. Whoever bought this information may send me free samples of the type of meat I am inferred to prefer, and may for instance place 'advertorials' on websites that I visit,[18] containing scientific evidence of specific health benefits of the consumption of beef. The profiling software may have calculated that such measures will reduce the chance that I stop eating meat by 23 per cent, thus making such investment worthwhile. Meanwhile, I am unaware of all this activity. Zarsky has named such interaction 'the autonomy trap': though I am making conscious choices, they are invisibly influenced by the knowledge asymmetry between those who profile and those who are being profiled.[19]

Autonomy is closely related to privacy, partly because privacy seems to be a precondition for autonomy. To make up one's mind, a person needs a measure of

17 Robert Merton popularised the Thomas theorem by referring to it as the ground for 'the self-fulfilling prophecy': R. K. Merton, 'The Thomas Theorem and The Matthew Effect' (1995) 74 *Social Forces* 379.

18 An advertorial is a blend of an advertisement and an editorial, or 'an advertisement that imitates editorial format' (Merriam-Webster dictionary at http://www.merriam-webster.com/dictionary/advertorial (last visited 28 December 2009)).

19 Zarsky, n 6 above.

freedom in the sense of not being constrained or forced by others to make one choice rather than another. Though privacy is often defined in terms of isolation and secrecy (the right to be left alone, or negative freedom), it has also been understood in a more fundamental way as the capacity to sustain the borders of one's person in relation with the social environment.[20] Here, privacy is seen not merely as a private interest but also as a precondition for informed citizenship and thus as a public good. From such a perspective, privacy is both relational and interactive and an important enabler of positive freedom.[21] Profiling has implications for privacy in several ways. First, it may generate knowledge about a person's lifestyle and preferences that most would consider rather invasive, violating the borders of one's personal identity. Second, it enables the use of such knowledge in order to 'manipulate' a person into choices she may have resisted had she been aware of what is known about her. Third, a person may be confronted with knowledge about herself that she was not aware of in the first place — such as specific health risks — that will have a major effect on her sense of self. There is ultimately a risk that the subliminal adaptations of the Ambient Intelligence environment in the end turn concepts like privacy into an empty shell, or as an illusion in the face of how the environment gradually creeps under a person's skin. Below we will explore this issue further by linking privacy to identity construction, arguing that the kind of personal identity that is presumed in constitutional democracy depends on a measure of opacity of individual citizens that may be lost in the era of smart machine profiling.

Discrimination and stigmatisation

Though errors and privacy are obvious vulnerabilities of Ambient Intelligence, there is also a pervasive threat of discrimination that is unjustified or unduly stigmatising. Profiling is a form of pattern recognition that affords refined forms of discrimination. In itself, discrimination is not a bad thing; indeed, it seems a truism that life depends on discrimination in the sense of detecting 'differences that make a difference'.[22] The law does not forbid discrimination per se; it provides remedies against unjustified or unfair discrimination. With unjustified discrimination we refer here to discrimination on the basis of inaccurate categorisation, as dealt with in the section on errors. This is not necessarily unlawful. We also use unjustified in the legal sense of discrimination on the basis of ethnicity, gender, age, without a valid ground for justification – which constitutes unlawful discrimination. With 'unfair discrimination' we refer to discrimination that is morally wrong because it deprives people of equal opportunities or burdens them with additional risks. This may or may not be unlawful. A salient example of the type of discrimination that is made possible by profiling

20 A. Westin, *Privacy and Freedom* (New York: Athenaeum, 1967); F. Schoeman, *The Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge UP, 1984).

21 Negative freedom (liberty) is defined as *freedom from* and positive freedom as *freedom to*: I. Berlin, 'Two concepts of Liberty' in I. Berlin, *Four essays on Liberty* (Oxford: Oxford UP, 1969/1958) 118.

22 G. Bateson, *Steps to an Ecology of Mind* (New York: Ballantine, 1972) 315. Bateson was one of the founding fathers of cybernetics, claiming that the core of cognition is locating relevant differences.

(2010) 73(3) 428–460

technologies is price discrimination, which allows businesses to charge different prices, depending on what they assume people are willing to pay for a good or a service. Consumers in different geographical areas can be offered different prices, based on differences in average income; consumers with different professional backgrounds can end up paying very different prices for similar products based on different spending patterns. Neo-liberal economists generally favour the idea of price discrimination because it allows a person to pay the exact price she is willing to pay. However, market conditions are seldom ideal, and price discrimination may be the result of information asymmetries; as soon as people find out who is paying less, they will refuse to pay a higher price.[23] Autonomic profiling technologies take the problem to a new level, as it becomes practically impossible to detect price differences where transactions are executed at a subliminal level and the categorisation that affords price discrimination is invisible for those who are profiled. The information asymmetry that causes a market failure in the case of price discrimination is equally problematic when other types of discrimination are at stake.[24] Certain goods or services may simply not be offered to a person, because she is assumed to lack the resources to invest in them based upon the 'knowledge' of how she is likely to distribute her income; low-quality products may be offered to a person because she is assumed not to have the time or the intelligence to do a product-comparison or because she is supposed to lack the money for better quality. Although such mechanisms have long been at play in consumer societies, the subliminal proactive profiling of Ambient Intelligence is likely to increase unfair discrimination practices exponentially.

What strikes us here is that whereas the technology of the written and printed word creates an ambiguity and delay that provides occasion to contest whatever is written down, the real time subliminal decisions taken by the Ambient Intelligent infrastructure seem to rule out the reflection that is typical for modern legal systems.[25]

Undue process

One of the most fundamental vulnerabilities generated by proactive environments is the threat to due process, though it is rarely discussed in the context of profiling. As a core principle of the rule of law, due process entails more than the

23 See A. M. Odlyzko, *Privacy, Economics, and Price Discrimination: Proceedings of the 5th International Conference of Electronic Commerce, ICEC 2003* (Pittsburgh: ACM, 2003) 355. Zarsky, however, argues that price discrimination can be a way to distribute costs between the rich and the less advantaged; under specific conditions this may be more fair than charging the same price for everyone: cf T. Z. Zarsky, 'Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society' (2004) 58 *University of Miami Law Review* 1014. The drift of his argument is, however, that data mining favours a different type of discrimination that is undesirable.

24 See Lyon, n 11 above.

25 See M. Hildebrandt, 'Law at a Crossroads: Losing the Thread or Regaining Control: The Collapse of Distance in Real-Time Computing' in M. Goodwin and B. J. Koops (eds), *Tilting Perspectives on Technology Regulation* (Nijmegen: Wolf, forthcoming).

fair trial of article 6 of the European Convention on Human Rights and its meaning is also not exhausted by the Fifth and Fourteenth Amendments to the US Constitution.[26] Due process in this broad sense refers to the opportunity to contest governmental actions in a court of law by whoever claims that her interests have been harmed, and stipulates that the remedy must be an effective one. In line with this notion, due process can be understood as the principle that empowers citizens to contest any decision that has a significant impact on their life and/or has legal consequences. Whereas the fair trial requires a specific and detailed articulation of the principle of due process (presumption of innocence, publicness, equality of arms, independence and impartiality of the judge, immediacy of the proceedings in court), in a more general way due process entails that a person has access to an effective remedy where she feels that her interests have been harmed. Steinbock gives the example of his library account being blocked. When he inquired at the 'help'-desk, they could not explain the block, leaving him with the inability to borrow books. A friend in the library's computer department was eventually able to tell him that the blocked account was due to mistaken identity, which had seen him identified as someone who was late in returning books. As the process was automated and the help desk had no access to the inner workings of the system, he could not contest the decision.[27] Steinbock convincingly argues that data mining and data matching could effectively rule out due process unless it is built into the socio-technical architecture. In the case of the library, this would be relatively easy. With the kind of real-time dynamic profiling that is a necessary part of Ambient Intelligence, however, it becomes much more difficult to incorporate the desired transparency into the system. Some authors have coined this approach 'values in design',[28] meaning that a value, norm, or principle is inscribed into the infrastructure in the design stage instead of adding it later. Indeed, adding such protection at a later stage will be costly and may thus be a competitive disadvantage, especially if we leave this kind of protection to the market. Citron has similarly argued for a more innovative way of thinking about due process in the face of automated technological infrastructures.[29] We will return to this point in more detail in the section on translating legal norms into technical code.

26 Fifth Amendment: 'No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.' Fourteenth Amendment: 'No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.'

27 D. J. Steinbock, 'Data Matching, Data Mining, and Due Process' (2005) 40 *Georgia Law Review* 1.

28 M. Flanagan, D. Howe and H. Nissenbaum, 'Embodying Values in Design: Theory and Practice' in J. van den Hoven and J. Weckert (eds), *Information Technology and Moral Philosophy* (Cambridge: Cambridge UP, 2008).

29 D. K. Citron, 'Technological Due Process' (2007) 85 *Washington University Law Review* 1249.

ADDRESSING THE THREATS I: CURRENT APPROACHES

The failure of privacy and data protection law

The previous section shows the multiple threats that practices of data collection, storage, mining, and profiling pose to citizens and consumers in the information society. Though existing law offers various instruments to counter such threats on the basis of traditional legal remedies we find them to be utterly inadequate in the face of this new information age. Currently, the key mechanisms for legal protection in this area are privacy and data protection law. To assess the potency of the existing remedies, it is useful to distinguish between these related but distinct concepts. Privacy is an interest, or value, consisting of several dimensions, including spatial (eg inviolability of the home), relational (eg protection of family and intimate life), and informational privacy. The latter is also known as data protection, suggesting that data protection is a subset of privacy, namely, privacy with respect to personal data. However, data protection is in fact a broader notion than informational privacy, since not all personal data are privacy-sensitive. For example, in many contexts providing a name or address does not infringe one's privacy; yet such information is nevertheless defined as personal data and must therefore be processed in line with data protection legislation. This conceptual movement can be viewed as circles in a Venn diagram, with a large overlapping area as well as distinct areas of their own. In the European context, data protection is indeed explicitly geared towards two different goals: the free flow of information within the internal market of the EU, but only where it is in accordance with the rights and obligations spelled out in the European Data Protection Directive (D95/46/EC). These rights and obligations aim to protect against more than just violations of informational privacy; they also aim to counter information asymmetries between individual citizens and data controllers, and to empower the first to negotiate with the second on the basis of a measure of transparency.

Privacy and data protection are well-established constitutional rights.[30] However, many authors agree that despite these protections, current law fails to provide sufficient protection against the threats outlined above. First, data protection law does not apply to many stages of the data mining and profiling process.[31] Most profiles are not traceable to unique persons and hence do not involve personal data that are subject to data-protection law. Indeed, for many types of profiling, it is not necessary to process uniquely identifiable data: data that correlate not at the individual level but at a more generic level or that are anonymous will suffice. This implies that profiling practices, at least at several stages of the profiling process, can disregard data-protection checks and balances such as correction or

30 See, notably, European Convention on Human Rights, Art 8; European Charter of Fundamental Rights, Arts 7 and 8; US Constitution, Fourth Amendment. Note, however, that for the US the scope of data protection in the Fourth Amendment is significantly limited by the third-party doctrine: cf D. J. Solove, *The digital person: technology and privacy in the information age* (New York: New York UP, 2004) 200.

31 M. Hildebrandt, 'Profiling and the Identity of the European Citizen' in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen* (Berlin: Springer, 2008) 326.

access rights, resulting in the relative opacity of both the profiling process and the resulting profiles. The only relevant provisions are articles 15 and 12 of the Data Protection Directive. Article 15 provides for the right of a person not to be subjected '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, such as his performance at work, creditworthiness, reliability, conduct, etc.' Article 12 provides a data subject with the right to obtain 'knowledge of 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'. Although these rights seem pertinent to the situation of a smart environment, paradoxically they are unhelpful precisely because they are entirely at odds with the intended subliminal autonomic character of Ambient Intelligence. Further, as stated in the preamble of the Directive, the concerned group profiles may be subject to intellectual property rights or be considered as a trade secret, meaning that a data subject may be denied access to the processes and profiles applied to him.[32]

Secondly, and more importantly, even where regular data protection law does apply to data processing because an identifiable data subject is involved, or because automatic decisions are implicated, data protection law turns out to be significantly flawed. Comparative evaluations of data protection legislation reveal significant gaps in legal protection. A recent survey of data protection law in the 27 EU member states – with arguably the world's strictest data-protection regimes – found that 'in various countries (eg BG, DK, LV, NL, PT, SK, RO), a gap exists between the protection of privacy related rights in the books, which may formally even conform to the requirements of EU and international law, and its protection in the law in action.'[33] This seems to confirm that the written law may be a paper dragon in the age of the 'digital tsunami'. One major problem is the disregard of the basic duty to register with the Data Protection Authority prior to engaging in data processing operations, with the consequence that supervision of data processing is impossible. As profiling processes are frequently covered by trade secret provisions or intellectual property rights, and because the technology may be a black box even for the data processor, adequate supervision of the duty to register is unachievable. Moreover, even where violations of data-protection provisions emerge, they are seldom punished with effective sanctions.[34] More often than not, non-compliance with data protection law does not occur deliberately but is caused by a lack of knowledge or understanding of the legislation, since the rules are unknown, ambiguous, vague, or too complex to be compre-

32 Recital 41: 'Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15(1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information'.

33 F. Fabbrini *et al*, *Comparative Legal Study on Assessment of Data Protection Measures and Relevant Institutions* (Florence: EUI, 2009).

34 *ibid.*

hensible.[35] Measures that currently attract much attention for addressing data-protection violations are security-breach notification laws.[36] Although such legislation requires organisations to notify customers or other relevant data subjects if personal data have been compromised the effect of such laws on overall actual data-protection practice remains to be seen.[37]

In addition to the serious gaps in data protection law, privacy law that looks beyond informational privacy shows similar deficiencies. For example, legislation on the inviolability of the home and integrity of the body is ill equipped to deal with certain developments in technology, such as domotics and wall- and clothes-penetrating cameras.[38] Similarly, innovations like smart metering, intended to collect precise information on energy use in order to provide energy-reduction advice to consumers, do not merely go against the grain of data protection regulations but also transgress the inviolability of the home and the protection of family life, insofar as it leaks information to third parties on in-home activities.[39] And as with data protection, in domains like police, national security,[40] and employment, privacy protection suffers when courts notice a violation of data protection but decide not to attach legal consequences to this finding.[41]

The gaps in legal protection are systemic

The gaps identified in the previous section in the legal protection offered by privacy and data protection law are not necessarily insurmountable, nor are they all new. The law, after all, continually faces challenges posed by new developments, not least where technology is concerned. Long-standing mechanisms to update the law – either by the legislator or the courts – will no doubt help to redress some of these failings. The problem, however, goes deeper than individual gaps. In our

35 *ibid*; see also C. M. K. C. Cuijpers and B. J. Koops, 'How Fragmentation in European law Undermines Consumer Protection: the Case of Location Based Services' (2008) 33 *European Law Review* 880.

36 California was the first state to introduce such legislation: see California Security Breach Information Act, California Civil Code § 1798.82; most other US states followed suit. In Europe, the Directive on Privacy and Electronic Communications D 2002/58/EC was amended by Directive 2009/136/EC of 25th November 2009 (inserting paragraph 3 in art. 4 of D 2002/58/EC) to specify a data breach notification to the competent national authority and, '[w]hen the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay'.

37 Boer and Grimmius, n 36 above, 15–16, quoting the only empirical study to date as finding a 'marginal [decreasing] effect' of 2 per cent on the incidence of identity theft (Carnegie Mellon University, *Do Data Breach Disclosure Laws Reduce Identity Theft?* September 2008).

38 B. J. Koops and M. M. Prinsen, 'Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution' (2007) 16 *Information & Communications Technology Law* 177.

39 E. L. Quinn, 'Privacy and the New Energy Infrastructure' (15 February 2009) at http://ssrn.com/abstract=1370731 (last visited 28 December 2009).

40 Note that public security and criminal justice are excluded from the applicability of Directive 95/46/EC in art 3(2).

41 See C. M. K. C. Cuijpers, 'Employer and Employee Power Dynamics: The Division of Power between Employer and Employee in the case of Internet and e-mail Monitoring and Positioning of Employees' (2007) 25 *John Marshall Journal of Computer & Information Law* 37; *Khan* v *United Kingdom* [2001] 31 EHRR 45.

view, privacy and data protection law are challenged at a more fundamental level by the developments in data mining and profiling: the flaws in legal protection are systemic. The data-protection principles and data-protection laws that have been established since the 1970s were based on the assumption that data processing should be kept to a minimum in order to prevent the misuse of personal data. Under these rules only a minimum amount of data is to be collected (the data minimisation principle) and to be processed solely for the purpose for which they were collected (the purpose-specification and purpose-limitation principles). It is questionable whether these assumptions still hold in the information society. Data storage devices and data networks create vast opportunities for data processing and profiling against diminishing costs, while the business models of e-commerce thrive on data analysis. The further integration of online and offline activities foreseen in scenarios portrayed in the report The Internet of Things will reinforce this commodification of data to the extent that personal data will in fact become the new currency.[42] Current legal protection disregards the fact that the value of data will entirely depend on an organisation's capacity to mine the data, due to the fact that without data mining tools it will not be possible to distinguish between noise and information. In this context, the principles of data minimisation and purpose limitation seem to miss the point.

We conclude that the current European legal framework is to some extent inadequate for today's world. Moreover, in a future dominated by Ambient Intelligence, protections based on informed consent or a right not to be subjected to automated decisions seem hopelessly maladroit; indeed, the whole point of Ambient Intelligence is to cater proactively and subliminally to the users' inferred preferences.

The US approach to data protection, which has always been more flexible than the European approach, has suffered from a similar major flaw since the Supreme Court's post-Katz adoption of the 'secrecy paradigm'[43] as the focus of the Fourth Amendment's privacy protection.[44] This paradigm determines that there is no reasonable expectation of privacy in data held by third parties since it has already been revealed to others and hence is no longer secret. As a result, such records are outside the scope of Fourth Amendment protective standards such as a warrant or probable cause. In a database nation, this doctrine arguably poses in the words of one scholar, 'one of the most significant threats to privacy of our times'.[45] Although the actual extent of the threat posed by the third-party doctrine is a topic of academic debate,[46] a more fundamental mechanism is at work through the concept of the 'reasonable expectation of privacy' that lies at the heart of the constitutional protection of privacy in the US. In Europe, where this concept is not as explicitly developed in case-law by the European Court of Human Rights, the concept does play a key if sometimes implicit role, particularly in the assess-

42 International Telecommunications Union, *The Internet of Things* (Geneva: ITU, 2005).
43 Solove, n 30 above, 200.
44 *United States* v *Miller* 425 US 435 (1976).
45 Solove, n 30 above, 202.
46 eg O. S. Kerr, 'The Case for the Third-Party Doctrine' (2009) 107 *Michigan Law Review* 561, 595, who describes various 'doctrines [that] limit considerably the threat that the third-party doctrine poses to civil liberties'.

ment of whether a privacy infringement is 'necessary in a democratic society'; this test is passed more easily when reasonable expectations of privacy are lower.[47]

What is at issue here is that information technology has an almost naturally eroding effect on privacy, since it tends to systematically lower the expectations we can reasonably entertain of keeping aspects of our lives private: as technology evolves, we gradually adapt ourselves to it, thus slowly transforming the reasonable expectation of privacy as well.[48] At the core of the mechanisms that lead us to believe that the gaps in data protection and privacy law are systemic, is the fact that the existing legal protection is embodied in written legal rules that cannot adequately cope with the real time pervasive and proactive technological infrastructure that may emerge. We are dealing with data processing that takes place on an enormous scale, instantaneously, ubiquitously, and in a multitude of ways that elude human observation. In this era, law in the books has reached the limits of its protective powers. As a result, a piecemeal, band-aid approach will not suffice to address the gaps in legal protection identified above.

Towards legal protection through 'code as law'?

A possible solution to the systemic gaps in legal protection is to use technology itself to enforce legal rules. There is nothing new in such a suggestion: the transformation of oral traditions into scribal societies (the era of the hand-written manuscript) and modern states (the era of the printing press) has demonstrated the plasticity of law, ambulating from a spoken to a written law.[49] Several authors have now begun to contemplate the next migration from written law to computer-coded law. In other words, besides the East-Coast code of Washington, DC – law codified in the books – legislators could use the West-Coast code of Silicon Valley software to articulate law in digital technologies.[50] The topos of 'code as law', as put forward by legal scholars such as Joel Reidenberg and Lawrence Lessig,[51] implies that digital technologies can be designed to support specific legal norms, inducing compliant behaviour. 'Code' or 'architecture' is the fourth of Lessig's four modalities of regulation: laws, norms, markets, and computer code. This modality of

> [c]ode is increasingly being sought as a regulatory mechanism in conjunction with or as an alternative to law for addressing societal concerns such as crime, privacy, intellectual property protection, and the revitalisation of democratic discourse.

47 cf S. Nouwt *et al*, *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy* (The Hague: Asser, 2005).

48 B. J. Koops and R. Leenes, '"Code" and the Slow Erosion of Privacy' (2005) 12 *Michigan Telecommunications & Technology Law Review* 115; D. J. Phillips, 'Privacy and Data Protection in the Workplace: the U.S. Case' in Nouwt *et al*, n 47 above.

49 R. K. L. Collins and D. M. Skover, 'Paratexts' (1992) 44 *Stanford Law Review* 509; H. J. Berman, *Law and Revolution: The Formation of the Western Legal Tradition* (Cambridge, Mass: Harvard UP, 1983); P. H. Glenn, 'Legal Cultures and Legal Traditions' in M. Van Hoecke (ed), *Epistemology and Methodology of Comparative Law* (Oxford: Hart, 2004) 7.

50 Lessig, n 15 above, 53.

51 *ibid*; J. R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 *Texas Law Review* 553.

Lessig argues in relation to privacy that technology 'has already upset a traditional balance. It has already changed the control that individuals have over facts about their private lives'.[52] To address this, the 'code' that disturbs the traditional balance between privacy should be checked by 'code' that incorporates privacy values.[53] Lessig is not alone in a call to engage digital technology itself to address the threats it poses. Since the 1990s, the need for creating and employing Privacy Enhancing Technologies (PETs) has been stressed by a growing number of legal scholars and information-security scientists as well as policy makers.[54] By embodying privacy rules in the technology that might otherwise afford invisible and gross transgressions of data protection principles, the relevant rules seem to translate seamlessly into the desired behaviours: the technology takes care of this by default.

There are two specific problems with using PETs to address the challenges raised by Ambient Intelligence, however. The first is that they are simply not used on a wide enough scale; despite the best efforts of privacy advocates, they have not moved beyond the stage of being a 'promising concept'. Although certain PETs, such as anonymisers, 'cookie crunchers', RFID blockers, and anti-spyware tools, are available on the market, since their employment is left to the market and service providers have no incentive to invest in them, consumers have to make an effort to search them out and spend the extra money to protect their privacy. Moreover, PETs diminish the functionality of the technology, for instance by slowing down the service, making their use less attractive. Further, precisely because users are often not aware of the covert data collection taking place within computer networks, they have no incentive to make the extra effort to protect themselves. In addition, the problem is compounded by the fact that to know which data one needs to hide, one needs to know the profiles one matches and the consequences of such matching.[55] To be effective, privacy enhancing 'code' should be default, meaning that it should be embedded in the infrastructure itself. Even where that is the case, however, PETs must be complemented with transparency-enhancing tools so as to provide users with knowledge of how they are being categorised and anticipated. Only then will citizens be able to make sensible decisions about which data to share. However, so far, the interests at stake in the power balances of commerce and government, as well as cost, convenience, and the stress on controlling security risks altogether all favour privacy-threatening technology far more than privacy-friendly 'code'.[56] The incentive structure to provide effective legal protection seems absent.

52 J.P. Kesan and R.C. Shah, 'Deconstructing Code' (2004) 6 *Yale Journal of Law & Technology* 277, 279.
53 Lessig, n 15 above, 142.
54 Registratiekamer (Netherlands) *et al*, *Privacy-enhancing Technologies: The Path to Anonymity* (Rijswijk: Registratiekamer and Information and Privacy Commissioner, 1995); European Commission, *Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228final, 02.05.2007; European Commission, *Privacy Enhancing Technologies: How to create a trusted information society. Summary of Conference* (London, 2007). For a philosophical analysis of the technological embodiment of values such as privacy, see Flanagan, Howe and Nissenbaum, n 28 above.
55 M. Hildebrandt (ed), *D7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools* (FIDIS, 2009) at http://www.fidis.net (last visited 28 December 2009); M. Hildebrandt, 'Who is Profiling Who? Invisible Visibility' in S. Gutwirth *et al* (eds), *Reinventing Data Protection?* (Dordrecht: Springer, 2009) 239.
56 Koops and Leenes, n 48 above.

The second difficulty with using PETs to address the privacy issues faced is that they do not tackle the challenges posed by smart infrastructures. As argued above, legal protection in the profiling era is not merely a question of hiding one's personal data. The shift in the collection and use of information outlined above has broad implications for public goods such as autonomy, non-discrimination, identity building, as well as the effective remedies to enforce such protection. If we are to protect citizens in the emerging information society, in which statistically inferred knowledge will play an increasing role, we need to draw a broader picture. To see what is required to address the vulnerabilities outlined above, we need a better understanding of how profiling affects our fundamental assumptions about democracy and the rule of law.

BACK TO BASICS: WHAT SHOULD LAW SAFEGUARD?

Privacy and identity in a constitutional democracy

Taking a closer look at the idea of rooting protection in 'code as law' reveals it to be a highly problematic solution. First, it depends upon market forces instead of legislative initiatives, thus lacking democratic legitimisation. Secondly, it seems to create a type of law that speaks for itself, ruling out the ambiguity that is inherent in spoken and written language; it is only capable of enforcing behaviour without, however, appealing to human reason or free will. In both cases, 'code as law' appears to replace the rule of law by a rule of technology. Brownsword has argued that forcing a person to comply with a legal rule fails the moral standards of what he calls a community of rights.[57] In fact, faced with the possibility of the rule of technology, he pleads for a fundamental right to violate the law, suggesting that without such a right the nature of law as we know it will change beyond recognition. We agree that in a constitutional democracy, law can neither assume compliance nor rule out non-compliance because citizens have the right to contest the law both when they vote for a new legislature and when they confront an alleged violation in court. They can claim that their action does not fall within the scope of a particular legal norm or that a particular legal norm is unconstitutional, for instance where it violates a human right. For this reason, code cannot become law unless it fits two requirements: first, it must be 'enacted' by the democratic legislature and second, it must provide the possibility of contestation in a court of law. These requirements constitute the difference between our concept of Ambient Law on the one hand and the technological enforcement of legal rules on the other. Ambient Law represents the technological articulation of legal norms as a form of democratic legislation, requiring both democratic participation and built-in safeguards that guarantee the contestability of the decisions made within the legal-technical infrastructure. The ambiguity of natural language and the written script have configured the law as a system of checks and balances that requires interpretation, and thus provides a space in which to

57 R. Brownsword, 'Code, Control, and Choice: Why East is East and West is West' (2005) 21 *Legal Studies* 1.

contest the dominant meaning. This space of contestation is the difference between mechanical compliance and autonomous action in accordance with the law and thus must form the central part of any response to a future 'Ambient' world.[58] Before turning to how that can be done, we first consider the notions of freedom and identity that are crucial for a constitutional democracy in a smart environment.

'Freedom to' and 'freedom from'

Historically, the freedom to participate in the public sphere is the oldest form of freedom, depicting the positive freedom to act, to influence one's fate and that of others. The idea that a person requires a measure of freedom from external constraints in order to make up her own mind is a recent invention, emerging from the beginnings of modernity.[59] This precondition can be found in the (Renaissance) humanistic approach to human action, stressing contextualism as well as individualism, born in the confrontation with other cultures and triggered by the seclusion of private reading that replaced public reading after the advent of the printing press. In a recent article, Stalder has explored the idea that our notion of privacy arose as a side effect of the practice of silent reading in one's private library, made possible by the printing press.[60] Private reading allowed one to travel in the mind, exploring different contexts and opposing visions of the good life, reconfiguring one's perspective to a unique blend of what was on offer as a result of the proliferation of printed material. Privacy as the 'right to be left alone' appears to stem from this type of negative freedom, vaguely reminiscent of Mill's warnings against the tyranny of public opinion.[61] Whereas democracy is sometimes confused with the dictatorship of the majority, the rule of law provides a safeguard against the imposition of majoritarian opinion on individual citizens. Constitutional democracy, then, is a system in which the majority rules subject to the duty to empower minorities to turn into majorities that can take over, until novel minorities reach a new majority. In a representative democracy, the freedom of an aggregated majority to rule is mitigated by the freedom from unnecessary constraints on the formation of opinions of individuals and minorities. Privacy, in this sense, though mostly associated with negative freedom, is an important precondition of the kind of positive freedom that is at stake in a constitutional democracy. This confirms that privacy is not only a private interest but also a public good that cannot be traded at will. The vulnerabilities generated by Ambient Intelligence, though not restricted to privacy, threaten privacy as a precondition for constitutional democracy, changing the very manner in which individual citizens engage in the reconstruction of their identities.

58 Hildebrandt, n 10 above; M. Hildebrandt and B. J. Koops (eds), *D7.9: A Vision of Ambient Law* (FIDIS, 2007) at http://www.fidis.net (last visited 28 December 2009).
59 See Berlin, n 21 above.
60 F. Stalder, 'The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy' (2002) 7 *Sociological Research Online* 141.
61 J. S. Mill, *On Liberty* (London: Penguin, 1974 [1859]).

'Idem' and 'ipse' identities

Agre and Rotenberg have defined the right to privacy in terms of boundary negotiations and identity building: 'the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity'.[62] What strikes us as pertinent here is that this definition combines negative and positive freedom; privacy as the freedom from unreasonable constraints actually allows for privacy as the freedom to build one's identity. Both types of freedom are seen as two sides of the same coin rather than as different interests. To understand how Ambient Intelligence and profiling technologies may impact identity construction, we need a more precise understanding of identity.

In his seminal work *Oneself as Another*, the French philosopher Paul Ricoeur discriminates between ipse and idem as two ways to understand identity.[63] Ipse refers to selfhood, while idem refers to sameness. Ipse is self-referential, it is about an 'I' (a first person singular) referring to herself (as if the self were a third person singular); ipse presumes a person who can reflect on herself as if she were another (from a third-person perspective). Idem is the result of an objectification, a comparison that allows a subject to establish sameness in the sense of similarity or even identicalness. In short, to look at oneself, one has to take the perspective of another; to look for sameness between different persons or to establish the objective identicalness of a person, a first-person perspective has to be assumed. The fact that our sense of self is constructed by looking back upon one's self from a distance, taking the viewpoint of another, implies that identity construction depends upon how we profile others to be profiling us. To be able to act, one needs to assess how one's behaviour is understood by others and what meaning they attribute to one's actions, which requires a double anticipation: the anticipation of how others anticipate us. The American pragmatist and social psychologist Mead actually spoke of this as our ability to take the role of the other, integrating different roles and interrelationships into what he called the 'generalised other'.[64] Identity-construction takes place in the midst of this anticipation, either rejecting the way we think others to be profiling us or embracing the way we are being 'identified'. In other words, identity building is the reiterative process of anticipated ascription and subsequent inscription.

As we have seen in the section on automated profiling, profiling is the enabling technology for smart environments. Ambient Intelligence depends on proactive servicing of individual citizens who have been categorised in terms of group profiles. What this means is that Ambient Intelligence anticipates and ascribes idem-identities to a person in order to be able to cater to her inferred preferences. Yet since Ambient Intelligence is about hidden complexity and invisible visibility, a

62 P. E. Agre and M. Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge, Mass: MIT Press, 2001). They build on the work of environmental psychologist Altmann, who developed a particularly relevant notion of privacy, integrating spatial and relational understandings of privacy, see I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Monterey: Brooks/Cole, 1975).

63 P. Ricoeur, *Oneself as Another* (Chicago: University of Chicago Press, 1992).

64 G. H. Mead and C. W. Morris, *Mind, Self, and Society from the Standpoint of a Social Behaviorist* (Chicago: University of Chicago Press, 1962).

person cannot easily guess or anticipate how she is being profiled. She may begin to respond to the idem-identities that are attributed to her without realising it, slowly incorporating them into her ipse-identity. To a certain extent this is nothing new, since we explicitly acknowledge that ipse-identity is always constructed in anticipation of the expectations, opinions, profiles, or stereotypes of others. The major concern here, however, is the fact that we have no access to these profiles. We cannot question them, contest their application, or amend their content as one can remonstrate with a human person who profiles us. Autonomic profiling unburdens us from taking a host of trivial decisions but also prevents us from engaging in the double anticipation that is necessary for the realisation of our negative and positive freedom. The reflection that was generated by the use of natural language, reinforced by the written and printed script, is absent from the process of seamless and ubiquitous adaptation that is generated by Ambient Intelligence.

ADDRESSING THE THREATS II: NEW APPROACHES

The importance of transparency

The double anticipation that is pertinent for the building of a person's identity requires a certain measure of transparency (of the group profiles used to categorise a person), as well as a measure of opacity (to allow a person to assess and to reject or embrace the profiles she anticipates). As Gutwirth and De Hert have argued, legal opacity tools as well as legal transparency tools are vital instruments in a democratic constitutional state. Both have the ultimate objective of limiting and controlling power. Whereas the right to privacy is primarily a tool to safeguard the opacity of individual citizens, data protection provides legal tools that guarantee the transparency of the actions of the state or other powerful players:

> The main aims of data protection consist in providing various specific procedural safeguards to protect individuals and promoting accountability by government and private record-holders. Data protection laws were not enacted for prohibitive purposes, but to channel power, to promote meaningful public accountability, and to provide data subjects with an opportunity to contest inaccurate or abusive record holding practices.[65]

According to Brin, transparency is one of the most fundamental pillars of the rule of law. It is a prerequisite for accountability, and 'accountability is no side benefit . . . Without the accountability that derives from openness – enforceable upon even the mightiest individuals and institutions – how can freedom survive?'[66] He argues that to stress privacy as the pièce de résistance of protection against technological threats may be picking the wrong battle, for it is difficult if not impossible to address the threats of the database nation and the profiling age by preventing and limiting data processing as this would require keeping the infor-

65 S. Gutwirth and P. De Hert, 'Regulating Profiling in a Democratic Constitutional State' in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen* (Berlin: Springer, 2008) 282.

66 D. Brin, *The Transparent Society: Will Technology Force us to Choose between Privacy and Freedom?* (Reading, Mass: Perseus, 1998) 13.

mation hidden by prohibiting the use of wall- and clothes-penetrating cameras, or any other new privacy-invasive technology. Given the unlikelihood of stopping the advent of such technology, he finds that a decrease in actual privacy is perhaps inevitable, but can be compensated by an increase in transparency:

> We may not be able to eliminate the intrusive glare shining on citizens of the next century, but the glare just might be rendered harmless through the application of more light aimed in the other direction . . . Transparency is not about eliminating privacy. It is about giving us the power to hold accountable those who would violate it . . . It may be irksome how much other people know about me, but I have no right to police their minds. On the other hand I care very deeply about what others do to me and to those I love.[67]

What others 'do' to Brin or to any other citizen of the information society is likely to be based increasingly on sophisticated group profiles that are used when decisions are made on whether or not to offer a service, to grant a request, or even to monitor a person suspected of plotting malicious actions. The consequences of these decisions can indeed be controlled by empowering those affected with the rights and means to resist them, providing what the European Court of Human Rights would call 'effective remedies' to contest decisions based mainly on statistical inferences. The prerequisite for this is that the relevant profiling and decision-making processes be made transparent.[68] Though we do not endorse Brin's unbridled belief in transparency as a panacea for the problems generated by the exponential growth of available data, we do think that for opacity tools to make sense in the era of profiling, citizens need to become much more aware of which data they wish to hide and consider the consequences of the data being leaked. Smart opacity thus requires transparency, both for its own sake (what is in the dark cannot be scrutinised) and for the sake of compensating the knowledge asymmetries that emerge in the wake of data mining society (since knowledge is power).

Adding TETs to PETs

As an instrument of safeguarding accountability, contestability and smart opacity, transparency cannot rely merely on law in the books.[69] Particularly in a world of Ambient Intelligence, there is a strong need to create transparency-enhancing technologies (TETs).[70] The main thrust of the idea of TETs is that Ambient Intelligence requires data optimisation, which is at odds with the logic of the current

67 *ibid*, 23 and 334.

68 '[I]n the case of automated decision making about individuals on the basis of profiles, transparency is required with respect to the relevant data and the rules (heuristics) used to draw the inferences. This allows the validity of the inferences to be checked by the individual concerned in order to notice and possibly remedy unjust judgements.' R. Leenes, 'Addressing the Obscurity of Data Clouds' in M. Hildebrandt and S. Gutwirth (eds), n 65 above, 298.

69 Legal realists have distinguished between 'law in the books' and 'law in action'; we paraphrase this distinction by contrasting 'law in the books' with 'law articulated in the technological infrastructure of Ambient Intelligence'.

70 See generally Hildebrandt, n 55 above.

data-protection regime and with the notion of PETs that require data minimisation. Smart applications depend on accessing as many relevant data as possible, while their relevance cannot be established in advance, especially in the case of bottom-up machine-learning techniques. As a result, these technologies will not function well in a scenario that is based on an individual hiding her data. Rather than merely trying to hide data to protect ourselves against surveillance and social sorting in an Ambient Intelligence world, legal and technological tools must be created that provide rights of access to or information about the profiles that can impact one's life. The effectiveness of legal tools must in fact be ensured by articulating them into the technological infrastructure they aim to protect against. While PETs 'think' in terms of shielding personal data, TETs 'think' in terms of empowering individuals by making profiling activities visible.

From the perspective of profiling technologies, the question of whether data are 'personal data' cannot be answered in advance because we never know what data will be correlated with other data and what knowledge will emerge from the processing of all or any data. At some point, anonymised data may be aggregated in a way that enables identification, turning previously anonymous data into personal data. As both the promises and the threats of Ambient Intelligence stem from the way in which data are processed rather than from the data themselves, we need to think in terms of dynamic, volatile, real-time profiles instead of stable personal data. Protection against abuse, misuse, or subliminal use of such real-time dynamic profiling depends on a measure of transparency. In the end, this transparency is a precondition of 'smart' opacity: to know which of your data you want to hide, you must know which profiles they match.

Thinking beyond Brin's plea for a transparent society in which privacy is given up in exchange for a nearly pervasive transparency, we argue for a smart type of data minimisation that is based upon a smart type of transparency. Instead of demanding access to profiles that are part of a company's trade secret or protected by means of intellectual property, the socio-technical infrastructure that affords autonomic profiling needs to be designed in such a way that it affords reasonably accurate anticipations of how a person is being and will be profiled. These anticipations must be as smooth, seamless, and subliminal as the smart environment itself, thus requiring novel types of human-machine-interfaces that warn a person how her behaviour may be interpreted by the smart infrastructure. This should allow her to play around with the network until she finds the right balance between opacity and transparency and between trust and control.[71] At the same time, the socio-technical infrastructure must provide a measure of transparency that allows for accountability of the data controller and/or data processor and for the contestability of the categorisations that have been applied. Access to an effective remedy needs to be available where a person has reason to claim a tort, a breach of contract, or unfair practices.

71 For examples of transparency-enhancing tools see *ibid*, chapter 5. See also eg D. H. Nguyen and E. D. Mynatt, *Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems* (Atlanta: Georgia Institute of Technology, 2002); D. Zwick and N. Dholakia, 'Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing' (2004) 24 *Journal of Macromarketing* 31.

A vision of Ambient Law

In an Ambient Intelligent future, say 2017, one could imagine the following scenario:

> David brings his daughter, Zoe, to school. After kissing him goodbye she enters the building. The building recognises her behavioural biometrics and turns on the screen of her virtual learning environment (VLE). By the time she reaches her desk, a program for the day is already on the screen: she will have to start with maths and then do some grammar. The program is based on her progress so far in relation to the end terms that have been set for this year, month, and week. After about half an hour, the program adapts to include fewer grammar exercises and more maths, because the VLE anticipates she will make better progress this way. Her interactions are monitored, her memory and understanding are tested, and she receives real-time feedback to speed up the learning process, this time applauding her efforts in maths. Her learning schedule for this week includes periods of intense interactive learning, regarding mathematics, the bio-natural sciences, the social sciences, infonomics, cognitics, and the arts. One of the mainstream techniques she works with is designing and testing simulations of 'natural' phenomena, foreign 'natural' languages, and history. This should provide her with an adequate sense of both the resistance of reality and the plurality of its manifestations. After some time, the VLE is shut off, tasking Zoe to get involved in real-world learning processes, and forcing her to stay tuned to her schoolmates, tutors, and the world outside the school. To the extent that Zoe learns to anticipate the VLE, she can tease out other responses by changing her behaviour. Thus she can prolong certain sessions and contest the feedback she receives.
>
> When she is allowed to re-enter the VLE, she presents herself to a peer group of pupils from different schools, categorised as having a shared background, need, or interest. She enjoys exchanging information on playing chess, one of her favourite pastimes, but she also shares information on how to tackle particular problems in her maths course in order to meet the targets set for this week. Though the VLE personalises her learning tasks to fit and elaborate her interests, it also confronts Zoe with the unexpected or undesired, in order to prevent the development of narrow and biased perspectives. Today, Zoe has to study and discuss the impact of animal testing on the researchers that perform the tests, a topic far outside her range of interest. All her personal data and profiles that are used to monitor her progress and adapt the learning environment to match her level of understanding are compiled in a protected virtual environment. The data can be mined anonymously for group profiling, including data from other schools. This has enabled a more refined understanding of a learning disability that Zoe suffers from, allowing the VLE to anticipate its negative effects by developing strategies to avoid whatever triggers the fatigue that blocks her capacity to take in more information. Again, to the extent that Zoe comes to understand how the VLE 'reads' her behaviour, she can influence the system's responses. This may actually speed up her learning process.
>
> When David enters to pick up his daughter, he asks her tutor to give him access to her personal profile. As he knows, he does not have unlimited access to her profile, and as she grows older, he will need her permission. This is not a problem to David, who is convinced of the importance of respecting his daughter's growing autonomy.[72]

72 This is a slightly adapted part of the scenario: see 'Once Upon a Time, in The Kingdom of Ambient Law' in Hildebrandt and Koops, n 58 above.

This scene is the third in a set of three future scenarios described in a report on Ambient Intelligence and Ambient Law. The first depicts a provider-centric and proactive environment; the second recounts a consumer-centric environment whose 'intelligence' is diminished by a persistent hiding of data and where convenience is hampered by a reoccurring need to give consent; while the third aims to balance proactive infrastructures by engaging the user in their operation. In place of either the data controller or the end-user actively using passive technologies, this last scenario shows citizens interacting with technologies;[73] and Ambient Law is targeted at precisely this shift from the use of technologies to interaction with technologies, allowing for proactive computing in a manner that sustains personal autonomy, and the measure of opacity and transparency it requires. This shift from use to interaction should not entail an unqualified celebration of Ambient Intelligence, but be grounded in a transformation that is constrained by legal principles designed into the code that 'runs' the system. For now, Ambient Intelligence is but a vision, albeit one in which the commercial sector and the European Commission are heavily investing; and as long as Ambient Intelligence is a research paradigm rather than an existing infrastructure, Ambient Law cannot be but a vision as well. However, to be well prepared for the dawn of smart environments, we think that the vision of Ambient Law requires a similar investment in time and human capital.

THE CHALLENGES OF MIGRATING LAW FROM BOOKS TO CODE

A migration from 'law in the books' to 'law in other technologies' is an important step towards safeguarding legal protection in the age of profiling. To achieve this migration, several challenges lie ahead. First, there is the technical challenge of sustaining the contestability of law in a constitutional democracy; to meet this challenge, rules must be embedded in such a way that they share the nuance and flexibility of the natural-language rules that determine the written law. Second, there is a democratic challenge: is value-embedded technology or the articulation of legal norms in digital technologies legitimate? Third, challenges of political-legal theory need to be addressed in order to prevent an uncritical embrace of 'digital law'.

The technical challenge: translating legal norms into technical code

Legal rules are formulated in human language and inscribed in the written and printed script, whereas 'code' rules are formulated in machine language. Despite decades of research into legal informatics, translating human-language rules into automated rules remains a daunting challenge. To give a mundane example: European law has envisioned the rule that lighters should be 'child-resistant', which means they are 'designed and manufactured in such a way that [they] cannot, under normal or reasonably foreseeable conditions of use, be operated by children

73 See E. Aarts and F. Grotenhuis, 'Ambient Intelligence 2.0: Towards Synergetic Prosperity' in M. Tscheligi *et al* (eds), *AmI 2009* (Berlin: Springer, 2009) 1; S. W. Brenner, *Law in an Era of "Smart" Technology* (New York: Oxford UP, 2007) chapter 7.

younger than 51 months of age'.[74] Various mechanisms can be used by producers to embed this rule in the architecture of the lighter, like 'Push in Lever', 'Force Only', or 'Spark Wheel Shield'.[75] But force-based lighters cannot recognise their user, and hence, ill, handicapped, and elderly people whose physical strength is failing may not be able to use them either. Complexity-based lighters are thus to be preferred from this perspective, but the regulation allows manufacturers to use only force-based mechanisms. The techno-rule thus is rigid: it does not allow for exceptions that the written legal rule allows. Moreover, there will be some 3-year olds strong or smart enough to use the lighter anyway. The techno-rule therefore is simultaneously over-inclusive and under-inclusive.[76]

Software code can of course be made more flexible, nuanced, and resilient than the architecture of a physical object such as a lighter. Code can also 'learn' from experience through the use of feedback loops and evolutionary programming. The 'ought' and 'permissible' operators of deontic logic are a welcome extension of the 'is' and 'not' of classic logic employed in computer science.[77] Nevertheless, machine language will still encounter difficulties in dealing with open norms like 'reasonable care' or 'necessary in a democratic society', which need to be interpreted with considerable attention to the context of a concrete case. This will require detailed refinements, specifying relevant circumstances and the weight that must be attributed to them. As Solum has suggested when discussing whether an artificial agent could act as a trustee,[78] difficulties will accumulate when discretion is at stake. Citron has similarly cautioned against 'translating' open legal norms into rigid technical code and her understanding of due process is particularly interesting for our vision of Ambient Law. Citron describes constitutional democracy as a system in which democratic rule-making is separated from individual adjudication, generating a system of checks and balances that provides for a legitimate and effective due process. She observes that:

> [t]his century's automated decision making systems combine individual adjudications with rulemaking while adhering to the procedural safeguards of neither . . . Code, not rules, determines the outcomes of adjudications . . . Last century's procedures cannot repair these accountability deficits.[79]

Citron, then, proposes a legal-technical framework to address some of these deficits, such as securing meaningful notice, protections for hearings, and transparency about the reformulation of legal rules that need to fit some of the inherent

74 Commission Decision of 11 May 2006 requiring Member States to take measures to ensure that only lighters which are child-resistant are placed on the market and to prohibit the placing on the market of novelty lighters (2006/502/EC), *OJ* L 198/41 of 20.7.2006, extended by Commission Decision of 12 April 2007 (2007/231/EC), *OJ* L 99/16 of 14.4.2007.

75 See Annex V of the Guidelines, 25 (with illustrations) at http://ec.europa.eu/consumers/cons_safe/prod_safe/gpsd/lighters/guidelines.pdf (last visited 28 December 2009).

76 cf L. Lessig, 'Law Regulating Code Regulating Law' (2003) 35 *Loyola University Chicago Law Journal* 1, discussing why 'regulation' by means of filtering technologies is both over-inclusive and under-inclusive.

77 See http://en.wikipedia.org/wiki/Deontic_logic (last visited 28 December 2009).

78 L. B. Solum, 'Legal Personhood for Artificial Intelligences' (1992) 70 *North Carolina Law Review* 1248.

79 Citron, n 29 above.

constraints of automated systems. Building on her work, we would suggest the need for measures such as requiring openness about the source code of systems whose decisions significantly affect citizens; rigorous and reiterated testing of such software systems, for example to check on a programmer's bias; developing ways to involve the public in the building of the automated systems that are going to regulate their lives; and refraining from encoding rules that require discretion to ensure just, equitable, and fair outcomes, taking into consideration contextual details that cannot be foreseen.

What should most interest us here is for lawyers to engage with the new socio-technical infrastructure and to seek solutions that involve the technologies themselves. Citron in fact provides a set of legal-technical remedies that would enhance the transparency of the system and allow for the contestation of its decisions. Evidently, the challenge is not merely technical, but also, and profoundly so, a legal one. Precisely for that reason, lawyers need to be involved to prevent inadequate reformulation of legal norms into technical architectures. This does not imply that articulating law in novel technological frameworks renders written law redundant. Just as written law has not replaced the role of unwritten law but complemented and changed it, written law as well as unwritten law will continue to play a key role in providing legal protection alongside Ambient Law.

The legal challenge: achieving legitimacy

Since Ambient Law consists of technically embedded norms intended to influence human behaviour, it should comply with criteria that society considers important for public regulation. Lessig argues: 'If code is a lawmaker, then it should embrace the values of a particular kind of lawmaking.'[80] First and foremost, the 'code' must be legitimate. Legitimacy has various dimensions in the context of 'code as law'; an extensive list of substantive, procedural, and result criteria can be drafted for assessing the legitimacy of a technology that aims to regulate human action. Substantive elements include, for example, human rights and moral values. Procedural elements relate to the rule of law, transparency of the rule-making process, and accountability; result criteria ensure that the rules should be flexible and transparent.[81] As with many categorisations, there is substantial overlap between them, if only because in the case of law procedural elements refer to substantive moral values (like fairness) and the law often disregards an outcome if it resulted from a violation of substantive or procedural norms. Legal rules articulated in the smart infrastructure may be devoid of transparency because default settings are invisible; they may be entirely inflexible because they simply enforce certain behaviours; and they may violate procedural norms of due process because users cannot contest their application. At a deeper level this raises a number of concerns with regard to their legitimacy.

80 Lessig, n 15 above, 224.

81 cf B. J. Koops, 'Criteria for Normative Technology: An Essay on the Acceptability of "Code as Law" in light of Democratic and Constitutional Values' in R. Brownsword and K. Yeung (eds), *Regulating Technologies* (Oxford: Hart, 2008).

As noted above, one major concern with 'code as law' is whether subjects retain the option of obeying or of disregarding the rule. If the articulation of the norm in technology is equivalent with the enforcement of the same norm – which is precisely the point of Lessig's 'code as law' – the moral framework of the law seems to crumble. As Brownsword has argued, an essential implication of human rights is that human beings should have a choice: the autonomy that underpins human rights 'implies the provision of a context offering more rather than fewer options'.[82] To safeguard the values of autonomy, self-development, and freedom, it is important not only that rightful choices are made (to comply with the rules) but also that wrongful choices can be made. Hence, it is important that disobeying or circumventing technologically embodied rules should remain possible. In the section on 'Privacy and identity in a constitutional democracy', we have referred to this as a fundamental right to violate the law.

Though we agree with Brownsword that enforcing lawful behaviour could strip the law of its appeal to human reason, it is important to note that legal normativity does not necessarily allow for violation, and that technological rules do not necessarily force our hand.[83] Though many legal rules are indeed regulative of human behaviour, some are constitutive, meaning that legal consequences hinge on compliance. One cannot be married if one violates the legal rule that the marriage is inscribed with the civil registry; one cannot own real estate if one is not registered as the owner in the relevant register. Similarly, some technologies regulate human behaviour: a speed bump inhibits speeding but it does not rule out driving too fast altogether. Other technologies are constitutive for human behaviour: digital rights management excludes certain types of behaviour unless one complies with the rules it intends to enforce.[84] The point is that legal rules – embodied in the technologies of the script – often cannot achieve the measure of compliance that rules embodied in speed bumps or computer code could.

This, however, is not necessarily the case, as it depends on the design of the technology in which a rule is articulated. A smart car that is capable of detecting a driver's fatigue can be designed as embodying either a regulative or a constitutive rule; if the fatigue detection exceeds a certain threshold, the car may either warn the driver or make driving impossible within a reasonable time interval.[85] Opposing 'law in the books' with 'technological implementation' wrongly suggests, first, that the former necessarily provides a type of freedom that the latter necessarily lacks; and, second, that technologies will be designed to enforce behaviour. With respect to the transparency of rules, Brownsword notes that even if regulation by means of technologies is implemented in a fully transparent and accountable way,

82 R. Brownsword, 'What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity' in R. Brownsword (ed), *Global Governance and the Quest for Justice. Vol. 4: Human Rights* (Oxford: Hart, 2004) 218.

83 M. Hildebrandt, 'Legal and Technological Normativity: more (and less) than twin sisters' (2008) 12 *TECHNÉ* 169.

84 The terms 'constitutive' and 'regulative' refer to Searle's distinction between 'brute' and 'institutional' facts, suggesting that normative rules can be regulative as well as constitutive for institutional facts, but only regulative for brute facts since these have been constituted by nature. See *ibid* for a more nuanced position on the difference.

85 S. Jin and S.-Y. Park et al, 'Driver Fatigue Detection Using a Genetic Algorithm' (2007) 11 *Artificial Life and Robotics* 87.

in due time transparency may be lost because the rule built into the infrastructure will simply become a part of its features and will no longer be recognised as a normative rule designed to influence people's behaviour. Then, it will be 'only outsiders and historians who can trace the invisible hand of regulation'.[86] Though written law suffers a similar fate when it becomes part of the social framework of a society, thus creating new habits that were initiated by the legislator, there is a serious challenge here. It regards the subliminal character of certain types of technological regulation and refers to the difference between the typical affordances of the script and those of a proactive environment. Whereas the script externalises the rule in a way that appeals to our conscious awareness, autonomic computing systems – like unwritten norms – seem to creep under the skin. The whole point of Ambient Law is to become aware of this and demand that digital regulation is designed in such a way that it is visible and contestable. This is precisely why the transparency of public regulation is such an important issue in Ambient Law. In fact, Ambient Law goes even further by requiring transparency for non-public regulation because it acknowledges that smart environments will regulate our lives in a myriad of ways – even if the designers think of this only as a side-effect.

The procedural legitimacy of Ambient Law requires more than the mere promulgation of techno-norms by a legitimate public law-making body. The vision of Ambient Law endorses a substantive notion of the rule of law rather than the formal notion of the 19th century 'Rechtsstaat'. Given our understanding of Ambient Law, the way in which a legal rule is translated and inscribed in a technology is a separate activity that should be assessed in its own right. As indicated in the previous section, the translation process from human to machine language implies choices and easily generates reductions, which potentially change the rule's content, scope, or effects. From the perspective of Ambient Law, it is exactly these choices that should be made in close cooperation with – if not simply by – public authorities, subject to democratic checks and balances.

Though all this may sound like science fiction to many lawyers and politicians today, Ambient Law requires a digital literacy of those who enact our laws (politicians) and of those who guard the internal and external coherence of our legal system (lawyers). Leaving such matters to technology developers that are at best subject to EDP auditors will make the mistake of viewing technology as a tool of implementation in place of acknowledging the extent to which it rules our lives. Yet, the embodiment of a rule in the technology of the script, or in another code, will change the nature of the rule. This calls for a new form of (digital) literacy and for the introduction of new checks and balances for the process of inscribing rules in Ambient Technologies.

The challenge of political-legal theory: participatory democracy

In light of the challenges outlined above, Ambient Law will require serious investments and it seems fashionable to respond to this with the admonition that

86 Brownsword, n 57 above.

a business case must be made for its feasibility. We contend, however, that if Ambient Law is left to depend on market forces, its success will depend on a power dynamic that does not necessarily reflect the public interest. Corporations will only embed legal protection in the architecture of their products on their own initiative if they have something to gain by its enforcement. Digital Rights Management systems have been swiftly developed over the past decade because the industry had much to gain by controlling the exercise of copyrights, whereas Privacy Enhancing Technologies remain a largely academic issue. Service providers usually have more interest in collecting data about their customers than in preserving their privacy. The default settings of the technical infrastructures, a primary regulatory tool in the hands of providers,[87] are generally based on the providers' preferences rather than on their users' interests, let alone on privacy and non-discrimination as public goods. With profiling technologies, particularly in an Ambient World, there seems no prima facie interest for Ambient Intelligence providers to address the vulnerabilities inherent in profiling for citizens and consumers. The business case for Ambient Intelligence rather dictates as wide a collection of data as possible. Thus without the intervention of the democratic legislator a provider-centric scenario for Ambient Intelligence seems much more likely than a user-centric or a 'smart' scenario with a significant level of transparency and user participation.[88] It is not the mere technological implementation of written law that is at stake, but the rather the enactment of legal protection in terms of the emerging socio-technical infrastructure. In the end, therefore, Ambient Law must be part of the political question as to how we can sustain the constitutional checks and balances for a viable democratic society.

This raises issues of political and democratic theory. Whereas the cynical question of 'Realpolitik' would be whether all this is politically and economically feasible, the normative question of legal and political philosophy is how we can learn to govern ourselves in a world of Ambient Intelligence. The answer to this question relates to how one understands democracy. The limits of traditional views on representative democracy, such as aggregative and deliberative models of representation, can be explored with a view to complement them with a more agonistic and participatory understanding of democracy.[89] The problem with aggregative models is that they often start from a methodological individualism that treats political choice as the result of the aggregation of given preferences.

The point is, however, that most people most of the time are not informed about most of the topics that warrant political decision-making. Their preferences in fact reflect their choice not to become involved, leaving the matter to their professional representatives. To develop an informed opinion they would have to enter into a discussion with stakeholders, experts and those who will be affected by the decisions made. This would turn them into a public, as defined by John

87 R. C. Shah and J. P. Kesan, 'Manipulating the Governance Characteristics of Code' (2003) 5 *Info* 3, 5–8; R. H. Thaler and C. R. Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness* (New Haven: Yale University Press, 2008).

88 See the scenarios in Hildebrandt and Koops, n 58 above; cf D.-O. Jaquet-Chiffelle (ed), *Identity R/Evolution* (FIDIS, 2009) at http://www.fidis.net (last visited 28 December 2009).

89 See M. Hildebrandt and S. Gutwirth, '(Re)presentation, pTA Citizens' Juries and the Jury Trial' (2007) 3 *Utrecht Law Review* 24.

Dewey in *The Public and its Problems*,[90] in which he explains that democratic publics are formed wherever people are no longer satisfied with how their government is dealing with their interests and decide to become involved. Instead of thinking in terms of one monolithic Public, whose interests can be reconstructed by means of rational deliberation, Dewey advocates the emergence of a diversity of publics around specific issues that actively participate in constructing and presenting a new common sense on the issues that concern them. From Dewey's perspective, democracy is an agonistic affair, bringing together advocates with different interests in the same 'matter of concern' to work out pragmatic solutions that are robust precisely because stakeholders in the broad sense have crossed swords over the issue whilst at the same time defining it.[91] His participatory understanding of democracy comes close to Mouffe's objections to the rationalist deliberative models of democracy: a viable democracy requires adversarial debates between a variety of proponents, rather than assuming that a rational consensus will result from rational deliberation.[92] It also accords well with Rip's arguments for an agonistic setting for what he calls constructive technology assessment.[93]

Whereas aggregative models of democracy assume that legitimacy derives from treating individual preferences as given, deliberative models assume that legitimacy derives from a rational reconstruction that will integrate incompatible positions into a rational consensus. Participatory understandings of democracy take into account that aggregative representation provides a general legitimacy that, however, needs contextualisation whenever preferences cannot be taken for granted owing to the invisibility of the consequences of decisions made, requiring a process of investigation as well as deliberation by those whose interests are at stake. Such an understanding of democracy also takes into account that rational deliberation can provide interesting analyses of moral, legal, and political concerns at a meta-level, but that these analyses nevertheless need to be tested against the voices of those whose interests are indeed at stake.

The relevance of Dewey's theory is pertinent here because it involves a rethinking of the traditional oppositions between experts and lay people and between expertise and experience. This is of particular importance in the case of Ambient Law. Publics must be formed by consumers, ICT enterprises, privacy advocates, consumer protection groups, computer engineers, scholars involved in STS (science, technology and society studies) and a great many other stakeholders, especially those whose interests will suffer or enjoy the direct or indirect consequences of the new socio-technical infrastructures. These publics should get involved in the legislative processes responsible for creating an incentive structure for smart environments that contain built-in checks and balances to protect the public goods of privacy, non-discrimination and due process.

90 J. Dewey, *The Public and its Problems* (Chicago: Swallow Press, 1927); N. Marres, *No Issue, No Public: Democratic Deficits after the Displacement of Politics* (Amsterdam: Rodolpi, 2005).

91 On the shift from 'matters of fact' to 'matters of concern', see B. Latour, 'From Realpolitik to Ding politik – or How to Make Things Public' in B. Latour and P. Weibel (eds), *Making Things Public – Atmospheres of Democracy* (Cambridge, Mass.: MIT Press, 2005).

92 C. Mouffe, *The Democratic Paradox* (London: Verso, 2000).

93 A. Rip, 'Constructing Expertise: In a Third Wave of Science Studies?' (2003) 33 *Social Studies of Science* 419.

Whereas a cynical 'Realpolitiker' may reject the feasibility of the Ambient Law we propose, the link between participative democratic theory and the growth of participatory Technology Assessment provides the opportunity to better understand how participating in rule-making implies partaking in the process of inscribing the rules in the relevant technological infrastructures. This will no doubt stretch the imagination of politicians used to doing their job by proposing and passing written laws, as it will probe lawyers' dependence on written text. At the end of the day, however, the need to establish an Ambient Law, as argued in this article, may be just the kind of catalyst required for law and politics finally to really take up the challenge of participatory governance.

CONCLUSION

The first question we addressed in this article was: what are the implications of the socio-technical infrastructure of Ambient Intelligence for privacy, identity, and the rule of law in a world of Ambient Intelligence? We have answered this question in terms of a set of vulnerabilities, starting with the more obvious threats such as those of inaccurate profiling and privacy, before outlining less visible threats such as the 'autonomy trap', unfair discrimination, and stigmatisation. The drawbacks of a smart proactive environment are generated by a novel type of knowledge, based on stochastic inferences rather than causal explanations or an understanding based on reason. These vulnerabilities are aggravated by the novel aspect of the subliminal level at which the adaptive environment responds to what it takes to be our preferences, building on an invisible visibility that is not open to contestation.

The second question we addressed was to what extent current law is able to address these vulnerabilities and how this relates to the law's current articulation in the technologies of the script. We have addressed this question by discussing privacy law and data protection legislation, finding that the emphasis on data minimisation and purpose limitation is at odds with the logic of autonomic profiling as this requires data optimisation instead. We concluded that the framework of privacy and data protection law is ill suited for an Ambient Intelligence world. Moreover, the real threats do not come from the collection or storage of personal data but from the application of group profiles that are protected as trade secrets or by means of intellectual property law. This indicates a pervasive lack of transparency that is systemic rather than incidental, and concerns the knowledge that is produced by data mining rather than what happens to one's personal data. The lack of transparency is not merely the result of systemic legal gaps, but also due to the ideal of hidden complexity that is part and parcel of Ambient Intelligence. The gaps in legal protection are therefore connected with the fact that modern law is embodied in the technologies of the script, facing serious interoperability challenges in meeting the demands of the emerging smart infrastructure. We thus propose a novel approach, coined Ambient Law, aiming to articulate fundamental legal protections into the socio-technical infrastructures that should enable Ambient Intelligence.

The third question we addressed was: in what ways should the law change to make the vision of Ambient Intelligence come true alongside a vision of Ambient Law that embeds fundamental values in the ambient profiling technologies? If we acknowledge the flexible character of law, how should we guide the necessary transformations of law's articulation into the novel socio-technical infrastructure? We have approached this question by building on Lessig's famous notion of 'code as law', while, taking heed of Brownsword's warnings against a rule of technology that could replace the rule of law. We emphasise that technological design is not necessarily deterministic, and point to technical solutions such as privacy-enhancing technologies that may be a first step towards something like 'code as law'. Other than the present undertakings in this regard, however, Ambient Law would also require the development of transparency-enhancing tools to render decisions taken by the smart environment contestable, if needed in a court of law. We also observe that in understanding privacy-enhancing technologies as mere instruments for the implementation of the law, their use is left to market forces that are not conducive to their uptake.

Thus, the challenge of Ambient Law is altogether far more fundamental than transposing 'legal' norms into 'technical' architectures. Ambient Law does not 'think' in terms of using technologies as neutral instruments to enforce the law, but as a novel way to articulate legal norms. This will require new levels of digital literacy of those who legislate – politicians – and of those who guard the coherence, the instrumentality, and the protective dimension of the law – lawyers. At the same time it calls for sensitivity on the part of both businesses and technology developers to the normative implications of these new socio-technical infrastructures, especially with regard to the checks and balances of democracy and the rule of law. Finally, we contend that this will require complementing traditional aggregative and deliberative models of democratic theory with a participatory theory that integrates recent experiments with participatory technology assessment.