This paper was presented at the symposium **REGULATION BY TECHNOLOGY** at the Netherlands Academy for Legislation, The Hague, on Friday 4th February 2011. A somewhat revised version has been published as:

'Legal protection by design: objections and refutations', (5) *Legisprudence* 2011-2, p. 223-248, available at http://www.ingentaconnect.com/content/hart/legis/2011/00000005/00000002/art00004

Challenges for a Vision of Ambient Law

Mireille Hildebrandt

> *To Microsoft, Kinect is not just a game, but a step toward the future of computing. 'It's a world where technology more fundamentally understands you, so you don't have to understand it'.*[1]

Abstract

To cope with an increasingly proactive technological infrastructure a so-called 'vision of Ambient Law' has been proposed. It entails that lawyers and legislators should learn to articulate legal protection into the digital environment. It implies that rights to privacy, due process and non-discrimination warrant effective remedies beyond the written law. The lawmakers' Pavlov response of introducing yet another set of administrative rules will not protect the inhabitants of smart environments, such as the Internet of Things or Ambient Intelligence. Neither will industry's self-regulation achieve adequate protection if citizens are not involved in the assessment of the infrastructure that enables proactive computation. Instead, an Ambient Law should be developed that enables 'legal protection by design'. This vision of Ambient Law builds on similar notions within the domain of ethics of technology (eg privacy by design, privacy by default, value-sensitive design).

Expanding on previous publications this paper engages with three possible objections. Firstly, some authors favour so-called technology-neutral regulations; they think that regulators should avoid technology dependence when formulating legal norms. Second, some authors might equate this approach with taking a 'command-and-control' perspective; they assume that the intervention of the democratic legislator actually implies a top down perspective, compared to e.g. public-private cooperation.

---

[1] Steve Lohr, "Computers That See You and Keep Watch over You," *The New York Times* January 1, 2011.

Third, some authors equate the idea of Ambient Law with technological enforcement of administrative law, suggesting that Ambient Law merely uses technology to enforce legal rules. I will argue that all three objections misconstrue the notion of Ambient Law, and miss the point that law-as-we-know-it is already technologically embodied. Moving from the technologies of the script to those of mobile interconnected digital computer systems requires creative re-enactment of legal norms into the novel infrastructures.

1 Proactive computational infrastructures: we are being 'read'

This contribution is focused on the legal implications of a novel socio-technical landscape that may have far reaching consequences for the way the law 'works'. The landscape I refer to is not merely a matter of digitalization (computers) or online connectivity (the Internet) but concerns the emergence of smart online and offline environments. Smart can mean many things, but here I will use the term to refer to computing systems that are capable of anticipating human behaviours on the basis of sophisticated statistical inferences. The computational 'intestines' of smart environments afford personalized services, based on pattern-recognition in big data-sets. If your data match a relevant pattern you will be profiled as having particular preferences, or as being prone to particular risks.

Behavioural advertising is a first sign of online personalisation and anticipation. It is based on extensive web statistics, such as those offered by Google Analytics.[2] This allows a website or an advertiser network to log all the behaviours of a website's visitors, including from which site or search engine they 'landed on' the site, how long they remain on a certain page, to what other pages they click, from which geographical location they arrive, what IP number they use, what other surfing behaviours they exhibit and possibly what keystroke and mouse-click behaviour they express (behavioural biometrics that render a person re-recognizable). This enables advertising networks to correlate all kinds of trivial online behaviour with online buying behaviour, thus providing advertisers with practical knowledge about their clients without a need for personal data such as name and address. As long as the profiler 'knows' what kind of person you are, and which offers might trigger your buying behaviours, advertisers can calculate which ads might bring them a profit.

Offline smartness is foreseen for 'smart homes', the 'smart grid', 'smart traffic management', 'smart offices' and the more.[3] The designers of Ambient Intelligence and the Internet of Things claim that these habitats will cater to our inferred preferences, capabilities or health-risks even before we become of aware of them.[4]

---

[2] Brian Clifton, *Advanced Web Metrics with Google Analytics*, 2nd ed., Serious Skills (Indianapolis, Ind.: Wiley Pub., 2010). See also the Opinion of the Art. 29 Working Party.

[3] Diane Cook and Sajal K. Das, *Smart Environments : Technologies, Protocols, and Applications* (Hoboken, NJ: John Wiley, 2005).

[4] Emile Aarts and Stefano Marzano, eds., *The New Everyday. Views on Ambient Intelligence* (Rotterdam: 010,2003), ITU, "The Internet of Things," (Geneva: International Telecommunications Union (ITU), 2005). ISTAG, "Scenarios for Ambient Intelligence in 2010," (Information Society Technology Advisory Group, 2001).

One day they might even predict a propensity for criminal conduct on the basis of correlatable data such as DNA, behavioural biometrics, emotion detection, long term health records and detailed school records. Hidden complexity, ubiquity, pervasiveness, seamless adaptation and proactive adjustment are the buzzwords of these novel infrastructures. They do not rely on 'stand-alone' devices but thrive on a continuous interconnectivity that allows for the capture and storage of an enormous amount of trivial data which are then mined for relevant patterns. Radio frequency identification (RFID) systems, combined with sensor technologies and wireless connectivity will provide 'big data' about mobility, temperature, facial expression, sound and speech, gait, one's history of previous behaviour in the same smart environment or even one's history of previous behaviours in other smart environments. They might even recognise emotional states from facial gestures or gait.[5]

The Kinect application is a good example of how the offline world will be 'turned online', as it communicates a person's physical behaviours in the form of machine-readable data to Microsoft's Windows Azure Platform to be further mined and analyzed.[6] The Kinect is a computer game that can be played by providing 'natural user input' such as voice and gestures, instead of a keyboard or joystick. The application uses a webcam and a microphone to collect machine-readable behavioural data of a user, which are then mined real-time in order to profile the user's interactions with what is on-screen. The Azure Platform is used to improve the software and further enrich the user experience. Note that the mantra for designing successful technologies has moved from 'increasing the functionality' to 'improving the usability' to 'augmenting or enriching the user experience'.[7] There is an acute awareness that for users to seamlessly interact with a smart application, they should not be asked to provide deliberate input via a separate interface but must be given the chance to employ the environment itself as an interface. Kinect shows what it means to directly interact with a smart environment, learning to anticipate how the application anticipates one's participation in an entirely intuitive manner. The communication between what happens on- and off-screen mainly takes place at a subliminal level, thus achieving a more smooth and 'natural' experience. This is how smart environments are meant to function, provoking effective mutual anticipations between a person and her smart environment, allowing her to participate in creating the intelligence of the system.[8] Instead of merely pre-empting a user and providing her with what she is inferred to prefer, there is a sustained interaction that unubtrusively engages a person as co-creator of a shared environment.

Despite the user-centric narrative about smart environments, many authors have doubts about what this means in practical terms. The emphasis on ubiquity,

---

[5] Rosalind Picard, *Affective Computing* (Cambridge, MA: MIT Press, 1997).

[6] The Kinect Privacy and Online Safety FAQs explain: 'Data collected through use of Kinect is stored on Microsoft's Windows Azure platform for up to three months, after which it will be deleted. During that three-month period, the data will be held for analysis purposes. If chosen for analysis, the data will be rendered into an anonymous state before use.' See http://www.xbox.com/en-US/Kinect/PrivacyandOnlineSafety#DataCollection7 (last visited 30 January 2011).

[7] See also Mike Kuniavsky, *Smart Things : Ubiquitous Computing User Experience Design* (Amsterdam ; Boston: Morgan Kaufmann Publisher, 2010).

[8] Emile Aarts and Frits Grotenhuis, "Ambient Intelligence 2.0: Towards Synergetic Prosperity," in *Ami 2009*, ed. Manfred Tscheligi, et al. (Berlin Heidelberg: Springer, 2009).

unobtrusiveness and the reiterated notion that these environments will cater to your wishes before you become aware of them seems to approach the human subject as an information object. Her preferences, life style, health and other risks are calculated based on advanced knowledge discovery in databases (KDD). To the extent that some of your relevant data match with patterns mined from these databases, you will be treated in a manner that is expected to fit your profile. Obviously this is not done for reasons of philanthropy but to persuade you to buy into the services offered by those who hope to make a profit by selling them. This sounds like as if the user is invited to participate only insofar as this will allow for more accurate predictions of her future behaviours, not to critically examine the correctness or the completeness of the profiles that underlie the way she is being served.

From the perspective of law and legislation it is important to note that smart environments require a networked technological infrastructure, whose computational complexity is hidden beneath the surface that 'acts' as the interface. There is a novel type of invisible visibility that pervades the ensuing mechanism of proactive servicing.[9] Whereas data analysis produces a new visibility of individual citizens based on the application of refined personalised group profiles, citizens themselves stumble upon a new invisibility. Both the software that creates personalised services and the group profiles it mines are protected by the law on trade secrets or that on intellectual property rights. Moreover, the complexity of the algorithms, neural networks or multi-agent systems involved obstructs an effective understanding of the bias and assumptions built into the models used for data mining.[10] Merely attributing transparency or privacy rights will not solve this problem.

2 Privacy, due process and non-discrimination

Much has been written about the legal and ethical implications of smart environments, notably on violations of privacy and refined and invisible forms of discrimination.[11] In this contribution I will briefly reiterate the argument that the usual interpretations

---

[9] M Hildebrandt, "Who Is Profiling Who? Invisible Visibility," in *Reinventing Data Protection?*, ed. S Gutwirth, et al. (Dordrecht: Springer, 2009).

[10] Technically speaking any type of data mining has inherent biases, meaning that any dataset can be mined in different ways with different outcomes. D Sculley and Bradley M Pasanek, "Meaning and Mining: The Impact of Implicit Assumptions in Data Mining for the Humanities," *Literary and Linguistic Computing* 23, no. 4 (2008).

[11] Jurgen Bohn et al., "Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing," in *Ambient Intelligence*, ed. W. Weber, J. Rabaey, and E. Aarts (Zurich: Springer, 2005), Daniel J. Solove, "Conceptualizing Privacy," *California Law Review* 90 (2002), Tal Z. Zarsky, ""Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion," *Yale Journal of Law & Technology* 5, no. 4 (2002-2003), David Lyon, *Surveillance as Social Sorting : Privacy, Risk, and Digital Discrimination* (London ; New York: Routledge, 2003). Andrew Odlyzko, "Privacy, Economics, and Price Discrimination on the Internet," in *Proceedings of the 5th international conference on Electronic commerce* (Pittsburgh, Pennsylvania: ACM, 2003). Anton Vedder, "Kdd: The Challenge to Individualism," *Ethics and Information Technology* 1 (1999), Bart Custers, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology* (Nijmegen: Wolf Legal Publishers, 2004). Helen Fay Nissenbaum, *Privacy in Context : Technology, Policy, and the Integrity of Social Life* (Stanford, Calif.: Stanford Law Books, 2010).

of privacy as individual *control over* or *restricted access to* personal information will not protect our privacy in a smart environment.[12] I will highlight the nexus between privacy, identity and some of the worries over social sorting and undesirable discrimination, while also noting that due process may be the biggest concern here.[13]

With regard to predictive profiling, there is a flaw in viewing privacy from the perspective of methodological individualism. The major problem is that it puts the burden of protecting privacy on the shoulders of individual inhabitants of smart environments, enabling them to trade their stake in what is also a public good. First, this flaw is connected with the pitfalls of regarding an individual as a sovereign in charge of disseminating personal data. Sovereignty assumes independence, both between states and within the state. Though this has been a very productive legal fiction in international law,[14] it is not – and never was - an accurate description of the nation state. Similarly, the control paradigm inherent in the idea of the person as a sovereign who rules her own thoughts, actions and decisions presumes an independence and a transparency that is not at hand. A large part of our inner life and interactions is co-constituted by unconscious processes and by the process of anticipating how others will 'read' our actions.[15] Nevertheless, acknowledging the relational and relative nature of individual personhood does not rule out a measure of autonomy that does make the difference between a person who can and an individual who cannot be called to account for her actions.[16] The problem with viewing a person as being in complete control over her personal information is that it denies the fact that all information is inherently relational: my name is of interest because others can use it to address me; Robinson Crusoe would not need or in fact 'have' a name insofar as he were to remain alone on his island. The fact that information is relational, however, does not imply that anybody necessarily has access to every bit of information that concerns me. Nor does it imply that I cannot hide information about myself or should not be able to prevent others from inferring information about myself that I could not possibly infer by myself. For instance, risk profiles based on how my DNA matches genomic profiles or on how my web-surf behaviour matches with customer profiles that determine credit worthiness may have a far reaching impact on my capabilities, though I may not be aware of this and therefore have no way of contesting their validity and relevance. Privacy as a form personal sovereignty may work in an environment where it is easy to foresee the consequences of sharing one's information; in a habitat that nourishes on information sharing and data correlation such a conception of privacy cannot protect us.

---

[12] E.g. M. Hildebrandt, "Profiling and the Identity of the European Citizen," in *Profiling the European Citizen. Cross-Discplinary Perspectives*, ed. M. Hildebrandt and S Gutwirth (Dordrecht: Springer, 2008).

[13] Cf. Daniel J. Steinbock, "Data Matching, Data Mining and Due Process," *Georgia Law Review* 40, no. 1 (2005).

[14] On the reality and force of legal fictions, see John Dewey, "The Historic Background of Corporate Legal Personality," *The Yale Law Journal* 35, no. 6 (1926).

[15] Ran R. Hassin, James S. Uleman, and John A. Bargh, *The New Unconscious*, Oxford Series in Social Cognition and Social Neuroscience (New York: Oxford University Press, 2005). On the double contingency that constitutes social interaction: Niklas Luhmann, *Social Systems* (Stanford: Stanford University Press, 1995).

[16] On the possibility of autonomy from the perspective of cognitive science: Antonio R. Damasio, *Self Comes to Mind : Constructing the Conscious Brain* (New York: Pantheon Books). From the perspective of moral philosophy: Judith Butler, *Giving an Account of Oneself*, 1st ed. (New York: Fordham University Press, 2005).

Second, this flaw relates to seeing privacy as a private interest, whereas it is *also* a crucial public good that in fact aims to *produce* a space for individuals to pursue their own interests. Privacy as a form of negative freedom (*freedom from*), is a recent invention. Historically speaking, positive freedom (*freedom to*) has been around much longer,[17] depicting the freedom of those engaged in political action as opposed to the *un*freedom of the private life that was constraint by the norms of the household (*oikos*). The idea that private life is a domain of liberty is a modern invention,[18] dating from the age of the printing press with its celebration of the silent reading of an increasing number of printed texts. In a way, the development of privacy as a means to retreat from social interaction is an affordance – some would say a side effect – of the era of the printing press.[19] Privacy in this sense cannot be taken for granted once the information and communication infrastructures are transformed from those of the printing press to those of the electronic age, the digital era, the profusion of interconnectivity and finally to those of the computational turn. Privacy as a public good is deeply entwined with the legal framework of constitutional democracy, as it aims to protect individual citizens from suffering the 'tyranny of public opinion' or the force of authoritarian government rule.[20] It is both *constitutive for* a resilient civil society and *constituted by* a legal framework that enables individual citizens to contest the way they are categorised, addressed or identified. Approaching privacy as a private interest easily ignores the fact that privacy depends on a social fabric and a legal framework that builds institutional gaps between different contexts, thus allowing a person to establish a dynamic and flexible multi-faced identity.

Agre & Rotenberg have defined the right to privacy as:

> The freedom from unreasonable constraints in the construction of once's identity.[21]

This is interesting for six reasons. First, this definition acknowledges that identity is not given, but the ephemeral result of a dynamic process. Second, it confirms negative freedom (*freedom from*) as the core of privacy, while – third – not every constraint is seen as a violation but only unreasonable constraints. Fourth, the constraints concern positive freedom (*freedom to*), thus providing a broader perspective to the concept of freedom instead of reducing it to the freedom to act arbitrarily. Fifth, the definition links privacy with the development of one's identity, while – sixth – understanding identity as inherently relational. This highlights the importance of context: who we are is co-determined by the context we engage with. If the context takes away the

---

[17] Isaiah Berlin, "Two Concepts of Liberty," in *Four Essays on Liberty*, ed. Isaiah Berlin (Oxford New York: Oxford University Press, 1969/1958).
[18] Hannah Arendt, *The Human Condition* (Chicago London: University Press of Chicago, 1958).
[19] Felix Stalder, "The Failure of Privacy Enhancing Technologies (Pets) and the Voiding of Privacy," *Sociological Research Online* 7, no. 2 (2002).
[20] John Stuart Mill, *On Liberty* (London: Penguin, (1859) 1974). Charles de Secondat Montesquieu, Thomas Nugent, and J. V. Prichard, *The Spirit of the Laws*, 2 vols. (New York ; London: Appleton, 1912).
[21] Philip E. Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: MIT,2001)., at 7.

possibility to foresee how we are being anticipated, the freedom to develop our identity is at stake.[22]

In the era of profiling this seems a more apt way to define privacy. The use of inferred profiles does not depend on personal data; the profiles are often inferred from anonymised data and do not refer to a particular person or even a particular group of persons. They usually concern non-distributive profiles, meaning that though the statistical inference is correct at the level of the dataset, it does not necessarily apply to those who fit the profile. This may sound counterintuitive but in fact it is not very surprising. If the average chance for all women to develop breast cancer is 12%, this does not imply that the chance to develop breast cancer is 12% for each and every woman. These chances will differ depending on other factors, such as genetic make-up, life-style, age and the more. If non-distributive profiles are applied to the inhabitants of smart environments their privacy may be implicated in several ways. First, to the extent that the profile is correct but the person is not aware of its content her capability to contest its relevance is denied. Second, to the extent that the profile is incorrect the person may end up responding to her treatment and thus reinforcing the profile. Paraphrasing Merton we could say that 'if machines define a situation as real it is real in its consequences'.[23] Precisely because smart environments thrive on subliminal interventions this might constitute a major invasion of a person's privacy in the sense of Agre & Rotenberg; the profiles that determine the proactive behaviours of the environment easily constrain the construction of identity in way that is unreasonable because incorrect and/or invisible. One's identity is unconsciously shaped by the continuous anticipations of smart fridges, intelligent filtering of incoming messages, adaptive traffic management or pre-emptive health monitoring. Dwyer has named this as the 'inference problem', which can be described as the fact that we are being 'read' whereas we don't know how and by whom we are being 'read'.[24] It related to the fact that though data protection legislation celebrates the purpose specification and the purpose limitation principle, ubiquitous computing and smart environments thrive on a productive function creep;[25] unexpected correlations that spring from bottom-up data mining will provide added value, they will keep the environment smart. Sticking to preconceived notions of what the purpose of a specific data mining operation will be would be against the paradigm of proactive and autonomic computing.

Being profiled in one way or another, correctly or incorrectly, wrongly or rightly, fairly or unfairly, also relates to the value of non-discrimination. Profiling is geared towards inclusion or exclusion in a very refined and sophisticated manner, thus allowing for personalised discrimination as to price, type and level of service, access to information, employment, healthcare or insurance. This type of discrimination is

---

[22] See also M. Hildebrandt, Who needs stories if you can get the data? ISPs and the ethics of big data crunching, paper presented at the seminar of 11th February 2011 on ISPs' responsibility, organised by Luciano Floridi, Oxford University.

[23] Robert K. Merton, "The Self-Fulfilling Prophecy," *The Antioch Review* 8, no. 2 (1948). This is referred to as the Thomas Theorem, cf. W I Thomas and D S Thomas, *The Child in America* (New York: Knopf, 1928).

[24] Catherine Dwyer, "The Inference Problem and Pervasive Computing," in *Proceedings of Internet Research 10.0* (Milwaukee, WI: 2009).

[25] Betsy Massiello and Alma Whitten, "Engineering Privacy in a Age of Information Abundance," in *Intelligent Information Privacy Management* (AAAI, 2010). at 120.

not new and much has been written about how everyday profiling basically springs from our bounded rationality, giving us a chance to use of our cognitive resources in an economical manner, and about how data mining allows for extensive price-discrimination that is not illegal nor always undesirable from the perspective of individual consumers.[26] The kind of discrimination that is at stake in smart environments is not necessarily related to the human right of non-discrimination and equal treatment, which refers to gender, race, ethnicity or religion. Nevertheless, profiling can easily create the means to discriminate people on the basis of trivial data that correlate with forbidden grounds of discrimination (called masking).[27] That way the discrimination is indirect and may be difficult to prove. However, the effects of being able to segment customers, tax-payers, job applicants, patients, offenders, suspects and citizens in general on the basis of non-distributive profiles has far reaching consequences that link discrimination with privacy. Being targeted as a certain type of person without knowing what the environment knows, could provide a person with a false sense of autonomy. Though she makes her decisions without visible constraints, the options have been formatted to fit her inferred inclinations. And to the extent that the environment decides on behalf of its inhabitants – like a discrete and well-trained butler – the inhabitants may actually begin to want what the environment has calculated to be their very own desire. Zarsky has coined this as the 'autonomy-trap'.[28]

At some point all these subliminal interventions could turn us into a cognitive resource for the smart environment, instead of the other way round. As with Kinect the environment may 'understand' us, whereas we have no clue about its mindless 'inner' workings, purposes or its machine-to-machine interactions with other smart environments. In this sense due process is the main problem. I use the term here to denote a person's ability to contest the way she is treated and to have equal access to 'knowledge' that determined how she was treated. In the tradition of art. 6 (concerning the fair trial) of the ECHR this is called 'equality of arms', meaning that a defendant is brought into a position that makes possible an effective defence. The computational turn that is a condition of possibility for smart environments creates a novel asymmetry of knowledge and information, even if this is 'sold' as hidden complexity, seamless interfacing and user-centric modelling. This knowledge asymmetry cannot easily be solved by means of written law. It requires a re-articulation of fundamental rights as defaults into the ICT infrastructure that could otherwise erase the possibility to exercise these rights.

---

[26] Frederick Schauer, *Profiles Probabilities and Stereotypes* (Cambridge, Massachusetts, London, England: Belknap Press of Harvard University Press, 2003). Odlyzko, "Privacy, Economics, and Price Discrimination on the Internet."

[27] Custers, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*.

[28] Zarsky, ""Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion."

3 Ambient Law: legal protection by design

In several publications the notion of Ambient Law has been put forward as a way to re-establish the Rule of Law in an Ambient Intelligent or smart environment.[29] In the context of a constitutional democracy the Rule of Law has at least two requirements. First, the scope and the content of the law are determined by a democratic legislator. Second, the final decision on what constitutes the correct interpretation of the law is in the hand of the courts. *Iudex – non rex – est lex loqui*.[30] This means that individual citizens have a means to challenge the administration's interpretation of enacted law, thus preventing a rule *by* law that employs the law as a neutral instrument to achieve the goals of policy makers. Instead, constitutional democracy entails that enacted law is seen as an instrument to achieve the goals of the democratic legislator, whereby the instrument embodies the constitutional constraints that are inherent in the Rule *of* Law. In other words, to count as *law* as opposed to mere *administration* or *discipline*, legal instruments must pass the test of aiming to achieve legal certainty, justice and purposiveness – even if it is clear that these goals may turn out to be incompatible in a specific case.[31]

The concept of Ambient Law (AmLaw) builds on notions such as value sensitive design, privacy by design and values in design.[32] It can be understood as 'legal protection by design'. I avoid terms like 'implementation' or 'enforcement' because AmLaw should not be mistaken for a rule by technology, merely using technological devices to enforce written legal norms. In fact I challenge the separation of means and ends that informs such a view of the relationship between law and technology.[33] Technology often has normative implications, also when they are not deliberately designed.[34] Though this is usually obscured by referring to these implications as side-effects, it reminds us that we must always carefully investigate to what extent a specific technology has affordances that interfere with the purpose for which it has been designed. Also, the affordances of new technologies may interfere with existing

---

[29] Mireille Hildebrandt, "A Vision of Ambient Law," in *Regulating Technologies*, ed. Roger Brownsword and Karen Yeung (Oxford: Hart, 2008), M. Hildebrandt and Bert-Jaap Koops, "A Vision of Ambient Law. Fidis Deliverable 7.9," (Brussels: FIDIS NoE (Future of Identity in Information Society, an EU funded Network of Excellence), 2007), M Hildebrandt and B.J. Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era," *Modern Law Review* 73, no. 3 (2010).

[30] K.M. Schoenfeld, "Rex, Lex Et Judex: Montesquieu and La Bouche De La Loi Revisted," *European Constitutional Law Review* 4 (2008).

[31] On means and ends: John Dewey, "The Logic of Judgments of Practice Chapter 14," in *Essays in Experimental Logic*, ed. John Dewey (Chicago: University of Chicago, 1916). On legal certainty, justice and purposiveness as the focus of law: Gustav Radbruch, *Rechtsphilosophie. Herausgegeven Von Erik Wolf* (Stuttgart: Koehler, 1950), Heather Leawoods, "Gustav Radbruch: An Extraordinary Legal Philosopher," *Journal of Law and Policy* 2 (2000).

[32] M. Flanagan, D. Howe, and Helen Nissenbaum, "Values in Design: Theory and Practice," in *Information Technology and Moral Philosophy*, ed. Jeroen Van den Hoven and John Weckert (Cambridge: Cambridge University Press, 2007), Marc Langheinrich, "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems," in *Proc. 3rd. Int'l Conf. Ubquitous Computing* (Springer, 2001). Batya Friedman, Peter H. Jr. Kahn, and Alan Borning, "Value Sensitive Desing and Information Systems," in *The Handbook of Information and Computer Ethics*, ed. Kenneth Einar Himma and Herman T. Tavani (New York: Wiley, 2008).

[33] Dewey, "The Logic of Judgments of Practice Chapter 14.".

[34] M. Hildebrandt, "Legal and Technological Normativity: More (and Less) Than Twin Sisters," *Techné: Journal of the Society for Philosophy and Technology* 12, no. 3 (2008).

legal norms, turning legal rights into paper dragons because it becomes increasingly difficult to exercise these rights. For instance, if the data protection directive D 95/46/EC provides a right of access to the logic of processing (art. 12) in the case of automated decisions, whereas it is technically impossible to provide such access in a way that is comprehensible for ordinary citizens, then the normativity that is inherent in the computational infrastructure will overrule the normativity of the written law. AmLaw suggests that to count as an effective remedy this legal norm will have to be inscribed at the level of the infrastructure, designing it in a way that provides adequate transparency in an intuitive way.[35]

Ambient Law takes into account that modern law has evolved from the information and communication infrastructure of the printing press, creating a body of written legal rules, written case law and doctrinal treatises that determines the substance of positive law. The systematic nature of modern legal systems builds on the need for systemisation, rationalisation and linear thinking that is inherent in the affordances of the printing press.[36] This has also triggered the growth of a class of legal professionals with the task of maintaining legal certainty in the face of proliferating legal texts (codes, cases, treaties and doctrine). The structure of modern law, with its emphasis on separate national jurisdictions, institutionalised appeal, constitutional review, *litis finiri oportet*, and the separation of legislator, administration and courts, has nourished the law as a relatively autonomous domain. This has eventually turned the rule *by* law that was typical for absolutism into the rule *of* law that is typical for constitutional democracy. Speaking of autonomous law does not, however, imply that law could ever function as a 'stand-alone device'. Rather, under the Rule of Law the legal system acts as a buffer between ruler and ruled, creating the possibility to contest state-authority in an appeal to a court that is in fact supported by the authority of the state (the paradox of the *Rechtsstaat*). Ambient Law acknowledges that all this cannot be taken for granted, because the Rule of Law is not only a historical artefact but also closely connected to a specific ICT infrastructure that may soon be overruled by another. If we want to sustain the rights and freedoms that developed with modern legal systems, legislators need to engage in the design of the novel computational infrastructures, taking care that they at least provide effective legal protection against their own omniscience and their capability to enforce a normativity that goes against the grain of constitutional democracy.

Hereunder I will discuss three objections against the vision of Ambient Law, hoping this will further clarify how Ambient Law relates to traditional written law and to technological enforcement of legal norms (which equals administration or discipline).

---

[35] The notion of an effective remedy has been elaborated by the ECHR, building on art. 13 of the Convention: Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

[36] References to Walter Ong, *Orality and Literacy: The Technologizing of the Word* (London/New York: Methuen, 1982). Elisabeth Eisenstein, *The Printing Revolution in Early Modern Europe* (Cambridge New York: Cambridge University Press, 2005 (second edition)), Jack Goody and Ian Watt, "The Consequences of Literacy," *Comparative Studies in Society and History* 5, no. 3 (1963). Pierre Lévy, *Les Technologies De L'intelligence. L'avenir De La Pensée À L'ère Informatique* (Paris: La Découverte, 1990).

4 Three potential objections

4.1 Technology-neutral legislation

There is an interesting debate on the extent to which legislation should be technology-neutral, and what this means. Several authors have pointed to the different meanings that underlie the policy-makers use of the concept.[37] Sometimes the concept is understood as relating to the goal of the legislation (non-discrimination, privacy protection, innovation, protection of intellectual property, ownership, retribution for a criminal wrong), but often enough it seems to refer to a general market-driven approach that sees legislation as a tool to stimulate innovation (rejecting legislation that discriminates between different technologies). Another goal is the wish to enact legislation that is 'future-proof',[38] not requiring reiterate adjustments when new technologies come to the market.

If technology-neutral legislation means that a legal norm should have similar effects independent of the technology involved, we need to acknowledge

> that technologically neutral rules addressing the same issue may well differ in their wording and content, in order to achieve the same (or at least broadly equivalent) effects when applied to these technologies.[39]

From this perspective, in drafting effective technology-neutral legislation the legislator can*not* afford indifference towards the available technologies; instead special attention is needed to avoid unwarranted consequences.

If technology-neutral legislation means that legal norms should not favour or discriminate between different technologies, in order to allow 'the market' to do its job, one could speak of 'technology indifferent laws'. However,

> Technology indifferent drafting may be an effective technique where the behaviour to be controlled, or the effects to be mandated or prohibited, are not made different in kind by the means adopted by the regulated actor. Where, though, the use of technology fundamentally changes the nature of the behaviour, or means that the effects of that behaviour are different or have different consequences, alternative mechanisms for achieving technology neutrality are required.[40]

For instance, within the domain of the criminal law one should only explicitly target particular technologies if they generate novel types of crimes or offences. It makes no sense to enact a new criminalization for killing a person by hitting her on the head with a personal computer, as it already falls within the scope of manslaughter or

---

[37] Chris Reed, "Taking Sides on Technology Neutrality," *SCRIPT-ed* 4, no. 3 (2007). B.J. Koops, "Should Ict Regulation Be Technology-Neutral," in *Starting Points for Ict Regulation: Deconstructing Prevalent Policy One-Liners*, ed. B.J. Koops, et al. (The Hague: TMC Asser, 2006). Reed, "Taking Sides on Technology Neutrality." Susan W. Brenner, *Law in an Era Of "Smart" Technology* (New York: Oxford University Press, 2007).
[38] Reed, "Taking Sides on Technology Neutrality." at 268.
[39] Ibid. at 267.
[40] Ibid. at 270.

murder. It does make sense to criminalize the hacking of a computer, because neither trespass nor theft entirely cover the act of entering a computer-system without the consent of its owner, perhaps also breaking the security and/or copying or even changing its content.[41]

What matters is that new technologies often afford actions and practices that were not possible before their invention. For instance, an e-book that allows the reader to search the entire book for particular words creates a type of transparency that was not available in a hardcopy, as this supports only a restricted version of such transparency by means of an index. The digital humanities have begun to discover how this affords entirely novel types of scientific research. Similarly, this kind of searcheability will at some point change the nature of legal research, for instance because it will allow data miners to come up with all kinds of abductive knowledge for classification, reasoning strategies and the like.[42] To the extent that new technologies have consequences that need redress which is not available within the existing legal framework it makes sense to address either their designers, users, retailers or end-users with legislation that clarifies ownership, tort or criminal liability, intellectual property rights or means of validation (e.g. in the case of the digital signature). In line with the systematic nature of modern law the legislator will attempt to tackle this by means of general norms that can be applied across different fields of application, serving the coherence of the legal framework and the legal certainty for individual citizens.

Ambient law is not concerned with enacting new legal norms in order to regulate new technologies. It is not about regulating computers, the Internet or smart environments. In that sense it is not cyberlaw or law in cyberspace. It does not focus on technologies as an object of regulation. Ambient law starts from the proposition that 'technology is neither bad nor good, but never neutral'.[43] From the perspective of philosophy of technology this means that it does not succumb to either techno-optimism or techno-pessimism; whether a particular technology is bad or good depends on which normative implications it has and how this is evaluated. This requires empirical research and moral assessment. The fact that technology is never neutral refers to the fact that any technology has normative force in the sense that is induces or enforces specific behaviour patterns and/or inhibits or rules out specific behaviour patterns.[44] The term normativity denotes more than mere regularity but less than morality: speed bumps generate slow driving, books generate silent reading, the Internet triggers peer-to-peer file sharing, the Forum Romanum generated a hierarchical distinction between speaker and audience, the Greek Agora triggered peer-to-peer discussions on the marketplace, artificial light generated longer working hours, Western music notation generated harmony and counterpoint, letters of credit generated trade beyond the local environment and finally generated paper money.[45] The normativity of technological

---

[41] See art. Cybercrime Convention.
[42] Reference Swansea conference.
[43] Melvin Kranzberg, "Technology and History: 'Kranzberg's Laws'," *Technology and Culture* 27 (1986).
[44] Hildebrandt, "Legal and Technological Normativity: More (and Less) Than Twin Sisters."
[45] This concept of normativity builds on Wittgenstein's notion of 'rule following', where 'rule' comes close to 'habit', see for instance Winch and Geertz, even if they seem to embrace a social constructivism that has no eye for technological normativity. Peter Winch, *The Idea of a Social Science* (London and Henley: Routledge & Kegan Paul, 1958), Clifford Geertz, "Local Knowledge: Fact and

devices or infrastructures does not depend on deliberate design; though people can delegate tasks to technology the 'real' workings often turn out different, since a technology usually affords more than its intended functionality. That is why AmLaw does not assume that technology is necessarily deterministic of human behaviour. Mostly, a technology can be engaged in a variety of ways, though at some point its usage is consolidated and people will tune their expectations to what turns out to be 'normal'. In that sense the normal or the 'default' has strong normative force,[46] though it must not be confused with moral force. Depending on its design a particular technology can overrule alternative action, forcing a person to act in a specific way. If a smart car will not start when the driver is under the influence of alcohol, it forces the driver's hand and is in that sense deterministic. However, if the car is design such that it warns the driver instead of overruling her action, it is not deterministic. In brief, Ambient Law does not regard technological infrastructures as necessarily deterministic, nor as inherently good or bad, but neither does it view them as neutral tools that can only be assessed in terms of efficiency and effectiveness.

Ambient Law is not concerned with technology as an object of regulation, but first of all with the prevailing ICT infrastructure as a *subject* of regulation (as a regulator). The computational infrastructure on which smart environments feed will regulate our lives in a number of ways: it will predict health and other risks, it will calculate our educational, occupational or professional capabilities, measure our resilience in the face of stress or exhaustion, predict the likelihood of violent behaviour or criminal offences and all this will allow the smart environment to unobtrusively include or exclude us from certain services, products, insurance, housing, education, profession and it will allow the smart environment to prohibit or provide access to physical or online domains. Note once again that the computational infrastructure will not force smart environments to act one way or another; there is no determinism here. But it would be very naïve not to acknowledge that these affordances change the playing field, the incentive structure and thus require us to re-install check and balances to counter undesirable defaults.

Ambient Law does not consider the ICT infrastructure that generates and channels communication and information flows to be a neutral tool. As an instrument of sharing and shaping meaning, enhancing and restricting the perception and cognition of individuals, groups, companies, governmental agencies and other organisations the ICT infrastructure is both constitutive and regulative of human societies. Moving from one type of infrastructure to the next has major consequences for the manner in which legal authority and normativity can be sustained. For lawyers and legislators it may be too obvious to note that modern law is in fact technologically embodied, namely in the technology of the script and the printing press.[47] It is even more

---

Law in Comparative Perspective," in *Local Knowlegde. Further Essays in Interpretive Anthropology*, ed. Clifford Geertz (New York: Basic Books, 1983).

[46] Richard H. Thaler and Cass R. Sunstein, *Nudge : Improving Decisions About Health, Wealth, and Happiness* (New Haven: Yale University Press, 2008). This relates to the notion of bounded rationality: Daniel Kahneman, "A Perspective on Judgement and Choice: Mapping Bounded Rationality," *American Psychologist* 589697-720 (2003).

[47] But see M. Ethan Katsh, *Law in a Digital World* (New York Oxford: Oxford University Press, 1995). and Ronald Collins and David Skover, "Paratexts," *Stanford Law Review* 44 (1992). Though perhaps Lessig made the most impressive analysis of the implications of Code's normativity, see my discussion of his work below Lawrence Lessig, *Code Version 2.0* (New York: Basic Books, 2006).

difficult to discover the implications of law's present focus on legal text and the subsequent implications of a shift towards images, sounds and things as interfaces that will replace, transform, augment and reinforce the role of printed text. As lawyers we have been so immersed in text that it has become a part of our identity, making it next to impossible to concede the materiality of law's present embodiment. Ambient Law aims to do just that. In admitting that its workings depend in part on the materiality of its technological embodiment Ambient Law challenges both lawyers and legislators to rethink what it means to create and sustain legal norms.

4.2 Top-down approach versus self-regulation?

One might think that the problems caused by the emerging computational infrastructure require either strong legal code or industry self-regulation to sustain core rights and freedoms such as privacy, non-discrimination and due process. Hirsch briefly sums up these positions:[48]

> Two main camps dominate the debate. The first calls for government regulation. It seeks legislation that would set, or authorize regulators to set, detailed and strict limits on the ways that companies can collect data online, the types and amounts of personal information they can collect, and on the ways they can use this data. Proponents of this approach maintain that strong government regulation is necessary to protect unsuspecting Internet users against the self-interested behavior of Internet-based companies. The second camp, which has thus far won the day, argues that the market and industry self-regulation will yield better results than government rules. It believes that Internet businesses already have a market incentive to protect user privacy so as not to lose customers. Insofar as rules are necessary to correct for market failures this group believes that industry, not government, should set them.

A number of objections can be made against the first option, as being a top-down approach or too slow or inflexible to provide adequate regulation of rapid technological change, or against the second option, as being a soft approach with a mistaken belief in free (but not necessarily fair) market self-regulation. Hirsch actually advocates a third approach, based on what he takes to be the European model of privacy protection: general and comprehensive data protection legislation, complemented by industry 'codes of conduct' that further interpret the scope and the implementation of the law, which are then made subject to government approval. He calls this co-regulation.

It is important to explain how Ambient Law relates to this opposition and to its synthesis. Firstly, Ambient Law is not about the implementation of legal norms by means of their technical enforcement. The technological infrastructure is more than a means to achieve an end. Having specific affordances it will co-constitute the scope and the consequences of the legal norm it articulates. Writing down unwritten legal norms is not a matter of implementing them, but rather concerns their articulation in a

---

[48] Dennis Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation," (2010).

specific technology: that of the script and the printing press. Similarly, the hardwiring and 'softwaring' of written legal norms would not be a matter of implementing them, but rather concerns their articulation in the technical infrastructure of the smart environment.

Second, just like the enactment of written legal norms, the articulation of legal norms in the novel infrastructure would require democratic legitimisation. If this were merely about technical implementation measures, the democratic element could be discarded as having been taken care of in the enactment of the written rule. As soon as we argue for the enactment of legal norms by articulating them in the novel ICT infrastructure, this will require democratic participation. Whereas in an oral culture democracy is a matter of consensual decision-making in a face-to-face assembly, scribal cultures often see the formation of proto-states where the literate class of scribes forms a buffer zone between ruler and ruled (which are often both illiterate).[49] The era of the printing press finally democratized literacy, enabling large polities to develop some form of representative and deliberative democracy. It may be that the era of interconnectivity warrants a further transformation of democracy that involves the novel infrastructure, especially the increasing always-on connectivity. Following a pragmatist account of democratic politics in the age of technological complexity, I would argue that the enactment of legal norms into an ICT infrastructure like that of smart environments would require participation of those who will suffer the consequences of relevant changes.[50] This could for instance be inspired by some form of participatory Technology Assessment or Constructive Technology Assessment.[51] Such novel forms of democratic participation could prevent Ambient Law from being imposed on designers, investors, providers and users of smart environments, requiring them to live with a technological fix that is invented by government officials.

As long as most lawyers and most legislators are not literate in terms of the computational infrastructure that nourishes smart environments we cannot expect them to come up with detailed and sustainable socio-technical solutions. In that sense Ambient Law cannot be based on a top-down format of democratic government. This, however, does not imply that we should resort to industry self-regulation, or combine such self-regulation with a general legislative framework (co-regulation). All three formats seem to understand the legislator as a typical governmental, top-down regulator and the industry as the actor whose behaviour must be regulated. From the perspective of democratic theory the legislator should not be reduced to a department of a top-down government structure but rather be understood – and empowered – as the embodiment of a people that speaks for and legislates for itself. As Hirsch demonstrates, many authors believe that giving the industry free reign has not worked, because there is no incentive to abandon profitable practices if one's competitors will then take over. A more attractive strategy could in fact be to engage

---

[49] H. Patrick Glenn, *Legal Traditions of the World* (Oxford: Oxford University Press, 2007 (third edition)).
[50] John Dewey, *The Public & Its Problems* (Chicago: The Swallow Press, 1927).
[51] "Tami: Technology Assessment in Europe: Between Method and Impact," (2004). Arie Rip, Thomas Misa, J., and Johan Schot, *Managing Technology in Society: The Approach of Constructive Technology Assessment* (London: Pinter Publishers, 1995). M. Hildebrandt and Serge Gutwirth, "Public Proof in Courts and Jury Trials: Relevant for Pta Citizens' Juries?," *Science Technology & Human Values* 33, no. 5 (2008).

the industry by levelling the playing field, thus allowing businesses to provide creative solutions to the requirements set by the legislator.[52] This sounds a bit like having your cake (good privacy standards) and eating it too (allowing business to innovate and come up with flexible solutions). The problem is that this assumes that citizens' privacy in a smart environment can be arranged between a top-down government and the industry. AmLaw is not only more ambitious in believing that democratic legislation is more than power politics between governmental and industrial stakeholders, it should for that same reason also be more effective.

Within the European context informational privacy is often seen as a form of informational self-determination, a term associated with the rulings of the German Constitutional Court and closely connected with the control theory on privacy.[53] Adding this to the previous analysis, we now have a quest for self-determination of the data subject, one for self-regulation of the industry, one for top-down regulation by the government and one for co-regulation between government and the industry. One does wonder how all this relates to the idea of self-government of a people (democracy) constraint by the rights and liberties of individual citizens (the Rule of Law). If government is there to represent its citizens then legislation must be a form of self-regulation; in a democracy legislation can only be top-down *after* being bottom-up.[54] What could it mean if the industry regulates itself in contravention of how citizens would like to rule themselves? And what could it mean if the industry regulates itself in ways that contravene individual rights and liberties? Do we assume that in practice the government and the industry operate outside the framework of democratic self-government and the Rule of Law?

Individual self-determination, top-down legislation and industry self-regulation are all based on some kind of sovereign rule; either by the self, the government or the industry. Co-regulation seems an uneasy negotiation between a sovereign state that knows best what the nation needs and a sovereign industry that knows best what the market needs. Considering what is at stake, we should not be surprised if government is compromised by giving in to tough negotiations, whereas leading partners in the industry find ways to reconfigure the market to their own advantage, with help of the government. Alternatively, government may outsmart other stakeholders and impose restrictions that smother innovation and subdue the economic miracles that e-commerce promises. All this sounds very familiar and pragmatic, but it is unclear how the deals struck in this context would benefit privacy as a private interest as well as a public good. The government obviously has its own reasons to invest in the computational turn to enhance its managerial efforts in the domain of e-government and to take care that the industry designs back-doors into its infrastructure for reasons of public security. If we stop attributing characteristics of the executive to the legislator which should in fact be a check on the administration, we may be able to

---

[52] It seems that the industry agrees that levelling the playing field is the only way that businesses can afford to turn privacy into a competitive advantage, see London Economics, "Study on the Economic Benefits of Privacy-Enhancing Technologies (Pets) - Final Report to the European Commission Dg Justice, Freedom and Security," (London: London Economics, 2010).

[53] BVerfGe 65, 1 (census decision).

[54] And the legislation that is imposed should also qualify as something that citizens could have preferred, cf. Jürgen Habermas, *Between Facts and Norms : Contributions to a Discourse Theory of Law and Democracy*, Studies in Contemporary German Social Thought (Cambridge, Mass.: MIT Press, 1996).

rephrase the issues in terms of the protection of privacy as a public good that cannot be traded with.

4.3 Rule *by* technology and the Rule *of* Law

Lessig must be credited with an impressive analysis of the consequences of novel ICTs for constitutional law, privacy, copyright and for the interrelationships between law, market forces, social norms and computer code. Writing at the end of the '90s, he highlighted the truism that law does not have a monopoly on the regulation of human behaviour, adding computer code to the list of influences on human behaviour patterns. In his famous *Code and other laws of cyberspace* Lessig pointed out that lawyers, courts and legislators should not take for granted that written law has an unmediated capacity to regulate especially if the architecture of our physical or virtual space sets defaults that nudge or force people in other directions. As a constitutional lawyer he emphasized the implications for the capacity of the law to safeguard constitutional rights and liberties, which brings his work close to my own concern for legal protection by design. I do find his distinction between law, market forces and social norms problematic, because these phenomena overlap. Market forces can be understood as being co-constituted by a particular type of social norms, deriving from institutional and legal constraints that co-constitute 'the market'. Legal norms that are not also social norms have difficulty to be sustained without continuous monitoring. This is not to say that all legal norms are also social norms, but especially in a democracy – where those who issue legal norms 'are' in a sense the same as those whose interactions should be guided by these norms – all legal norms are meant to become social norms.

Over and against the more usual 'command and control' model of law, which seems to have inspired Hirsch's notion of governmental regulation, Glastra van Loon developed an 'expectancy model' of legal norms.[55] He explains that legal norms (or rules) enable citizens to anticipate what behaviour both the government and their fellow citizens can legitimately expect from them. Van Loon distinguished between an imperative and a normative aspect of rules in general. In modern legal systems all legal norms have an imperative aspect, which is related to the positivity of law and its relation to government authority and the monopoly of violence. It means that in the end of the day citizens can call upon the government to enforce valid legal norms against their fellows. Under the Rule of Law legal norms can also be enforced against the government, which requires an internal division of sovereignty, allowing the courts to invoke government authority to call other parts of the government to account. The imperative aspect of legal norms entails a vertical relation between the issuer of a norm and the addressee. To 'work' however, legal norms must develop a normative aspect, which concerns the way subjects relate to each other. This plays out in the horizontal relationship between citizens who can call each other to account when specific legitimate expectations are not met. Under the Rule of Law the normative aspect also guides the relationship between citizens and government, who are *both* subject to the imperative force of legal norms. The fact that legal norms

---

[55] J.F.G. Glastra van Loon, "Rules and Commands," *Mind* LXVII, no. 268 (1958).

should generally have a normative aspect is not only related to their effectiveness but also to their legitimacy. As suggested above, in a democracy all legal norms are supposedly issued *by those to whom they apply*. The fictional character of this assumption is not fictional in the sense of imaginary, but in the sense of constructive; it is a productive fiction that requires legislation to live up to certain standards. The fiction entails a norm about the content of legislation: it should be composed or designed in a way that takes into account the serious concerns of all citizens, even if compromises must be reached.

How does the normativity that is inherent in technological artefacts or infrastructures relate to Van Loon's analysis? Should we understand the possibility of enforcing certain behaviour patterns as imperative, while qualifying the possibility to set defaults that can be side-stepped as normative? I think that this would confuse matters. Though the possibility to enforce behaviour can be termed deterministic for or constitutive of these behaviours, it has little to do with the imperative aspect. In law, we can also distinguish between regulative and constitutive rules. A constitutive rule means that when you violate it you cannot achieve your objective; in a sense you cannot violate the rule because in that case it refuses to attach legal consequences to your actions. In many jurisdictions you cannot be married without registering the marriage, violating this rule means that you are not married. A regulative rule like the prohibition of speeding or causing damage means that violation will be fined or will be followed by an obligation to pay compensation. Both rules have an imperative aspect, since they were issued by the legislator. Hopefully both rules have a normative aspect, meaning that people will feel obliged towards each other to take the rule as a standard. In the case of constitutive rules this may be even more important, because if many people 'get married' without registering their marriage the legal norm may lose its meaning as such and possibly erode the authority of the legislator. Technological normativity can be constitutive or regulative, but for such normativity to be complemented with an imperative aspect the norm must be enacted by the legislator. This means that the legislator *has paid explicit attention to the norm that is at stake*. Either the legislator has articulated a rule in spoken and/or written human language and discussed with computer scientists, engineers and designers how this rule can be articulated in the technological artefact that may otherwise counter the rule, or the legislator has decided that a particular technological device has normative consequences that require reconstruction or redesign to generate a normativity that does not violate constitutional safeguards.

In his inaugural lecture Leenes discusses what he calles 'technoregulation', which he defines as

> deliberate employment of technology to regulate human behaviour[56]

or

> technology with intentionally built-in mechanisms to influence people's behaviour.[57]

---

[56] R. Leenes, *Harde Lessen. Apologie Van Technologie Als Reguleringsinstrument* (Tilburg: Universiteit van Tilburg, 2010). at 21.

Leenes then differentiates between techno-regulation authored by the legislator and intrinsic techno-regulation, which he apparently defines as authored by a private actor. In line with his definition of techno-regulation he considers both as forms of deliberate, intentional regulation. This comes close to what Latour has called delegation: certain tasks are delegated to a technology that either forces or induces the targeted behaviour. As Leenes notes, as long as the initiative or the endorsement for such delegation is with the legislator there seems to be some kind of democratic legitimacy, whereas this is debatable when a private actor delegates his terms of service to a technology thereby extending his own control in a way that violates rights of the buyer or user of the service.

From the previous it should be obvious that the technological normativity that is the focus of this article is not necessarily part of techno-regulation. The problem with techno-regulation is that is restricts itself to intentional delegation whereas the normativity that is generated by proactive computational infrastructures may not have been intended. Ambient Law focuses on what we could call the normative affordances of the proactive computational infrastructure, without assuming that any one person or organization had the intention of inscribing such norms. We tend to define unintended consequences as side-effects, but one of the crucial implications of this novel infrastructure seems to be that it becomes hard to discern the consequences of one's actions – whether or not intended. Maybe the side effects will have a bigger impact than whatever were the intended effects. For Ambient Law to make a difference it should not restrict itself to techno-regulation but investigate the normative affordances of the infrastructure, before requiring alternative designs to protect citizens against violations of their constitutional rights.

This is also the reason why I prefer to speak of 'legal protection by design' instead of 'techno-regulation'. In using the term *legal* I emphasize the role of the democratic legislator as well as the possibility to contest the way the norm affects human behaviour. In using the term *protection* I emphasize that this is not about implementing written legal rules by means of technological enforcement. I also avoid the term regulation that easily resonates the top-down managerial governmental model discussed in the previous section. Finally, in using the term *design* I emphasize that this is not only about engineering but also about human-machine-interfacing, highlighting that such inscription of legal norms is not only a matter of technique but also an art.

Basically, I want to prevent a rule *by* technology that views technology as a neutral tool to achieve policy goals, which fits easily with seeing law as a neutral instrument. Neither law nor technology can be used as mere means to specified ends. This would reduce either of them to administration or discipline, as Leenes clearly shows. Neither rule *by* law nor rule *by* technology is what fits constitutional democracy. Rule by Law can incorporate articulation of legal norms in written law, in unwritten law and in hardwired/'softewared' law.

---

[57] B.-J. Koops et al., *Starting Points for Ict Regulations, Deconstructing Prevalent Policy One-Liners* (Cambridge: Cambridge University Press, 2006). at 158.

5 Closing remarks

In this contribution I contrast the notion of Ambient Law with Lessig's regulatory mix of market forces, social norms, legal code and computer code, with Hirsch's opposition between governmental command & control models versus self-regulation and with Leenes' discussion of techno-regulation.

To fine-tune the contrast I explore three well-known objections against regulation by means of technology, which may or may not refute the argument for Ambient Law. The first concerns the idea that legislation should be technology neutral and should therefore abstain from aligning itself with a particular technology. In reply, I have argued that technology neutrality must not be confused with technology indifference. Since modern law is already articulated in the technology of the script we must face the fact that the emergence of a novel information and communication infrastructure may render written law ineffective, especially in the case of the legal protection of human rights. The second is directed against using technology as a tool of legislation because it reinforces the command and control model of regulation, which is deemed to suffocate innovation and to create a host of problems with compliance. In reply, I have argued that seeing democratic legislation as a form of top-down command and control implies a flawed understanding of what constitutional democracy stands for. The top-down model of governmental rule is based on a problematic notion of sovereignty that fits the 18th century police state rather than states that embrace democracy under the Rule of Law. Though I do not deny that a democratic legislator may be hijacked by executive pressures or by transnational market forces, the way out is not to grant private stakeholders the freedom to design their own rules of the game. Instead, alternative, upstream democratic participation processes must be generated that allow stakeholders as well as citizens to get involved in the design of the novel ICT infrastructure. The third objection understands Ambient Law as a way of using technology to enforce legal norms, which would indeed be a form of administration or discipline rather than law. In reply I have argued that Ambient Law should steer clear of automated implementation of legal norms, and instead recreate an information and communications infrastructure that scaffolds the private and public autonomy of individual citizens.

6 Bibliography

Emile Aarts and Frits Grotenhuis, "Ambient Intelligence 2.0: Towards Synergetic Prosperity," in *Ami 2009*, ed. Manfred Tscheligi, et al. (Berlin Heidelberg: Springer, 2009).

Emile Aarts and Stefano Marzano, eds., *The New Everyday. Views on Ambient Intelligence* (Rotterdam: 010,2003).

Philip E. Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: MIT,2001).

Hannah Arendt, *The Human Condition* (Chicago London: University Press of Chicago, 1958).

Isaiah Berlin, "Two Concepts of Liberty," in *Four Essays on Liberty*, ed. Isaiah Berlin (Oxford New York: Oxford University Press, 1969/1958).

Jurgen Bohn et al., "Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing," in *Ambient Intelligence*, ed. W. Weber, J. Rabaey, and E. Aarts (Zurich: Springer, 2005).

Susan W. Brenner, *Law in an Era Of "Smart" Technology* (New York: Oxford University Press, 2007).

Judith Butler, *Giving an Account of Oneself*, 1st ed. (New York: Fordham University Press, 2005).

Brian Clifton, *Advanced Web Metrics with Google Analytics*, 2nd ed., Serious Skills (Indianapolis, Ind.: Wiley Pub., 2010).

Ronald Collins and David Skover, "Paratexts," *Stanford Law Review* 44 (1992).

Diane Cook and Sajal K. Das, *Smart Environments : Technologies, Protocols, and Applications* (Hoboken, NJ: John Wiley, 2005).

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

Antonio R. Damasio, *Self Comes to Mind : Constructing the Conscious Brain* (New York: Pantheon Books).

John Dewey, "The Historic Background of Corporate Legal Personality," *The Yale Law Journal* 35, no. 6 (1926).

———, "The Logic of Judgments of Practice Chapter 14," in *Essays in Experimental Logic*, ed. John Dewey (Chicago: University of Chicago, 1916).

———, *The Public & Its Problems* (Chicago: The Swallow Press, 1927).

Catherine Dwyer, "The Inference Problem and Pervasive Computing," in *Proceedings of Internet Research 10.0* (Milwaukee, WI: 2009).

London Economics, "Study on the Economic Benefits of Privacy-Enhancing Technologies (Pets) - Final Report to the European Commission Dg Justice, Freedom and Security," (London: London Economics, 2010).

Elisabeth Eisenstein, *The Printing Revolution in Early Modern Europe* (Cambridge New York: Cambridge University Press, 2005 (second edition)).

M. Flanagan, D. Howe, and Helen Nissenbaum, "Values in Design: Theory and Practice," in *Information Technology and Moral Philosophy*, ed. Jeroen Van den Hoven and John Weckert (Cambridge: Cambridge University Press, 2007).

Batya Friedman, Peter H. Jr. Kahn, and Alan Borning, "Value Sensitive Desing and Information Systems," in *The Handbook of Information and Computer Ethics*, ed. Kenneth Einar Himma and Herman T. Tavani (New York: Wiley, 2008).

Clifford Geertz, "Local Knowledge: Fact and Law in Comparative Perspective," in *Local Knowlegde. Further Essays in Interpretive Anthropology*, ed. Clifford Geertz (New York: Basic Books, 1983).

J.F.G. Glastra van Loon, "Rules and Commands," *Mind* LXVII, no. 268 (1958).

H. Patrick Glenn, *Legal Traditions of the World* (Oxford: Oxford University Press, 2007 (third edition)).

Jack Goody and Ian Watt, "The Consequences of Literacy," *Comparative Studies in Society and History* 5, no. 3 (1963).

Jürgen Habermas, *Between Facts and Norms : Contributions to a Discourse Theory of Law and Democracy*, Studies in Contemporary German Social Thought (Cambridge, Mass.: MIT Press, 1996).

Ran R. Hassin, James S. Uleman, and John A. Bargh, *The New Unconscious*, Oxford Series in Social Cognition and Social Neuroscience (New York: Oxford University Press, 2005).

M Hildebrandt, "Who Is Profiling Who? Invisible Visibility," in *Reinventing Data Protection?*, ed. S Gutwirth, et al. (Dordrecht: Springer, 2009).

M Hildebrandt and B.J. Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era," *Modern Law Review* 73, no. 3 (2010).

M. Hildebrandt, "Legal and Technological Normativity: More (and Less) Than Twin Sisters," *Techné: Journal of the Society for Philosophy and Technology* 12, no. 3 (2008).

———, "Profiling and the Identity of the European Citizen," in *Profiling the European Citizen. Cross-Discplinary Perspectives*, ed. M. Hildebrandt and S Gutwirth (Dordrecht: Springer, 2008).

M. Hildebrandt and Serge Gutwirth, "Public Proof in Courts and Jury Trials: Relevant for Pta Citizens' Juries?," *Science Technology & Human Values* 33, no. 5 (2008).

M. Hildebrandt and Bert-Jaap Koops, "A Vision of Ambient Law. Fidis Deliverable 7.9," (Brussels: FIDIS NoE (Future of Identity in Information Society, an EU funded Network of Excellence), 2007).

Mireille Hildebrandt, "A Vision of Ambient Law," in *Regulating Technologies*, ed. Roger Brownsword and Karen Yeung (Oxford: Hart, 2008).

Dennis Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation," (2010).

ISTAG, "Scenarios for Ambient Intelligence in 2010," (Information Society Technology Advisory Group, 2001).

ITU, "The Internet of Things," (Geneva: International Telecommunications Union (ITU), 2005).

Daniel Kahneman, "A Perspective on Judgement and Choice: Mapping Bounded Rationality," *American Psychologist* 589697-720 (2003).

M. Ethan Katsh, *Law in a Digital World* (New York Oxford: Oxford University Press, 1995).

B.-J. Koops et al., *Starting Points for Ict Regulations, Deconstructing Prevalent Policy One-Liners* (Cambridge: Cambridge University Press, 2006).

B.J. Koops, "Should Ict Regulation Be Technology-Neutral," in *Starting Points for Ict Regulation: Deconstructing Prevalent Policy One-Liners*, ed. B.J. Koops, et al. (The Hague: TMC Asser, 2006).

Melvin Kranzberg, "Technology and History: 'Kranzberg's Laws'," *Technology and Culture* 27 (1986).

Mike Kuniavsky, *Smart Things : Ubiquitous Computing User Experience Design* (Amsterdam ; Boston: Morgan Kaufmann Publisher, 2010).

Marc Langheinrich, "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems," in *Proc. 3rd. Int'l Conf. Ubquitous Computing* (Springer, 2001).

Heather Leawoods, "Gustav Radbruch: An Extraordinary Legal Philosopher," *Journal of Law and Policy* 2 (2000).

R. Leenes, *Harde Less. Apologie Van Technologie Als Reguleringsinstrument* (Tilburg: Universiteit van Tilburg, 2010).

Lawrence Lessig, *Code Version 2.0* (New York: Basic Books, 2006).

Pierre Lévy, *Les Technologies De L'intelligence. L'avenir De La Pensée À L'ère Informatique* (Paris: La Découverte, 1990).

Steve Lohr, "Computers That See You and Keep Watch over You," *The New York Times* January 1, 2011.

Niklas Luhmann, *Social Systems* (Stanford: Stanford University Press, 1995).

David Lyon, *Surveillance as Social Sorting : Privacy, Risk, and Digital Discrimination* (London ; New York: Routledge, 2003).

Betsy Massiello and Alma Whitten, "Engineering Privacy in a Age of Information Abundance," in *Intelligent Information Privacy Management* (AAAI, 2010).

Robert K. Merton, "The Self-Fulfilling Prophecy," *The Antioch Review* 8, no. 2 (1948).

John Stuart Mill, *On Liberty* (London: Penguin, (1859) 1974).

Charles de Secondat Montesquieu, Thomas Nugent, and J. V. Prichard, *The Spirit of the Laws*, 2 vols. (New York ; London: Appleton, 1912).

Helen Fay Nissenbaum, *Privacy in Context : Technology, Policy, and the Integrity of Social Life* (Stanford, Calif.: Stanford Law Books, 2010).

Andrew Odlyzko, "Privacy, Economics, and Price Discrimination on the Internet," in *Proceedings of the 5th international conference on Electronic commerce* (Pittsburgh, Pennsylvania: ACM, 2003).

Walter Ong, *Orality and Literacy: The Technologizing of the Word* (London/New York: Methuen, 1982).

Rosalind Picard, *Affective Computing* (Cambridge, MA: MIT Press, 1997).

Gustav Radbruch, *Rechtsphilosophie. Herausgegeven Von Erik Wolf* (Stuttgart: Koehler, 1950).

Chris Reed, "Taking Sides on Technology Neutrality," *SCRIPT-ed* 4, no. 3 (2007).

Arie Rip, Thomas Misa, J., and Johan Schot, *Managing Technology in Society: The Approach of Constructive Technology Assessment* (London: Pinter Publishers, 1995).

Frederick Schauer, *Profiles Probabilities and Stereotypes* (Cambridge, Massachusetts, London, England: Belknap Press of Harvard University Press, 2003).

K.M. Schoenfeld, "Rex, Lex Et Judex: Montesquieu and La Bouche De La Loi Revisted," *European Constitutional Law Review* 4 (2008).

D Sculley and Bradley M Pasanek, "Meaning and Mining: The Impact of Implicit Assumptions in Data Mining for the Humanities," *Literary and Linguistic Computing* 23, no. 4 (2008).

Daniel J. Solove, "Conceptualizing Privacy," *California Law Review* 90 (2002).

Felix Stalder, "The Failure of Privacy Enhancing Technologies (Pets) and the Voiding of Privacy," *Sociological Research Online* 7, no. 2 (2002).

Daniel J. Steinbock, "Data Matching, Data Mining and Due Process," *Georgia Law Review* 40, no. 1 (2005).

"Tami: Technology Assessment in Europe: Between Method and Impact," (2004).

Richard H. Thaler and Cass R. Sunstein, *Nudge : Improving Decisions About Health, Wealth, and Happiness* (New Haven: Yale University Press, 2008).

W I Thomas and D S Thomas, *The Child in America* (New York: Knopf, 1928).

Anton Vedder, "Kdd: The Challenge to Individualism," *Ethics and Information Technology* 1 (1999).

Peter Winch, *The Idea of a Social Science* (London and Henley: Routledge & Kegan Paul, 1958).

Tal Z. Zarsky, ""Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion," *Yale Journal of Law & Technology* 5, no. 4 (2002-2003).