© Banksy 2008, Corner or North Rampart and Kerlerec Streets, New Orleans·

THE RULE OF LAW IN CYBERSPACE?

22 December 2011
Inaugural Lecture Mireille Hildebrandt
Chair of Smart Environments, Data Protection and the Rule of Law
Institute of Computing and Information Sciences (iCIS)
Radboud University Nijmegen

A time is marked not so much by ideas that are argued about as by ideas that are taken for granted. The character of an era hangs upon what needs no defense.

Lawrence Lessig (2001)
The Future of Ideas, at 5

INTRODUCTION

In 2009 Malte Spitz requested access to his personal data from his telecom provider. After he had obtained a court order that compelled the provider to do so, he published them online in *Die Zeit*,[1] not as a long and boring list enumerating the more than 35,000 registrations, but visualised on a map of Germany and combined with data that can easily be found online. The young German politician thus showed how easy it is to acquire a detailed picture of someone's activities – who they are, what they do, and where and when they do it. All that you need are the personal data that internet and mobile phone users 'leak' unintentionally or provide deliberately. Telecom providers have this information, and law enforcement authorities can demand access to it under certain conditions.

In the summer of 2011, Max Schrems, a 23-year-old law student from Vienna, requested the European office of Facebook in Ireland to disclose which of his personal data they process.[2] Some time later, he received a CD from Facebook in California with 496 MB of data, equivalent to 1222 pages. Besides the sheer magnitude of the data, he was struck by two matters of concern: a great deal of data was missing, and the records still contained data that he had deleted. On 28 September, Facebook replied as follows with regard to the missing data:

> To date, we have disclosed all personal data to which you are entitled pursuant to Section 4 of the Irish Data Protection Acts 1988 and 2003 (the Acts).
> (…)
> Please note that certain categories of personal data are exempted from subject access requests.
> (…)
> Section 4(12) of the Acts carves out an exception to subject access requests where the disclosures in response would adversely affect trade secrets or intellectual property. We have not provided any information to you which is a trade secret or intellectual property of Facebook Ireland Limited or its licensors.

The Irish Data Protection Act contains two relevant articles, both based on the European Data Protection Directive. To begin with, the Act stipulates that we have the right of access to the logic involved in the automatic processing of personal data, especially when used for making decisions that significantly affect us.[3] However, based on a recital in the preamble to the Directive, the Act also stipulates that provision of such information is not required to the extent that is would adversely affect trade secrets or intellectual property.[4] In short, we have the right to know if and how the computational algorithms determine whether we can take out a life insurance policy or are eligible for credit, or whether we qualify for a good education or a job, but if that knowledge violates trade secrecy or the intellectual property of software or databases, that right will lapse. Or so it says in the Irish law. The Directive, however, qualifies this by adding that the protection of trade secrecy or intellectual property should not result in the data subject being refused all information.

In the quoted correspondence, Facebook suggests that our personal data could be subject to their trade secret or intellectual property rights. Obviously, this cannot be the case. They could, nevertheless, claim legal protection for the way in which our personal data are sorted in a database and the way knowledge is mined from the aggregate data. In this lecture I will argue that precisely these two aspects are going to change our relationship to reality and that they will have a major influence on the mode of existence of the law and the possibilities of sustaining the Rule of Law. My lecture thus concerns two aspects: the way in which our personal data are amassed with data from many others and the way in which a new type of knowledge is derived from this aggregate, as this is used for making all manner of decisions. Both techniques are part of the computational intestines of cyberspace. The aggregation and algorithmic searching of databases extends not only to commercial interests, but increasingly determines the interaction between government and citizens, particularly in criminal law and fraud detection (taxes, social security). In science as well, generating, aggregating and smart searching databases appears to have become the norm. Meanwhile, there is talk of a 'computational turn' in philosophy, science, business and society.[5]

PART I: MODES OF EXISTENCE

The issue evoked by the new computational order has far-reaching implications for the way we act, decide, perceive and know. This requires not only new legal rules or interpretations of existing law, but above all a prudent reflection on *the manner in which the law exists* and hence the relationship between law, state, technology and society.

Some will oppose the advance of information-driven systems, while others will embrace them as productive innovations. Still others will deny that there is anything new under the sun, or will state that technology has its own dynamics about which you – like the weather – can do little (except of course purchase an umbrella). My suggestion is that we buy a good umbrella and meanwhile identify and investigate the influence of the computational turn in science and society. I will return to the umbrella in my conclusion. Let us keep our distance from the idea that technology cannot be tamed, nor claim that it can easily be brought under our control. Indeed, technology often controls us, while we attempt to control it. Or, to cite the American philosopher of technology Don Ihde: new technology invents us, while we invent it.[6]

I also want to distance myself from gloomy pessimism or hallucinatory utopianism. Current technology – and therefore cyberspace – is not good or bad, but is never neutral.[7] As McLuhan pointed out, this has less to do with how a medium such as the printing press, television or the internet may be abused, but primarily with 'the change of scale or pace or pattern' that the medium introduces into human relationships.[8] These transformations depend on the design of the medium and the way it is taken up in everyday life. Latour, for example, reminds us that a man with a firearm is a different person than one without. He thus referred not so much to the psychological impact of carrying a firearm, but to its implications for the web of relationships that determine the existence of the person: for instance, lethal effect is possible at a greater distance than with a knife, and it is possible to shoot in ambush, where the shooter can strike without being seen. The introduction of firearms has had important implications for both warfare and for law enforcement as well as crime (whereby it is crucial whether citizens are allowed to carry such weapons or that, in principle, only the police can do so). Cyberspace not only triggered games like World of Warcraft, but is also the condition of possibility of drones (unmanned military aircraft that can be controlled remotely). As with firearms, the availability of drones changes the scale, distance and precision of tactical warfare and the mutual visibility (or invisibility) of the shooter and the target. In line with that it disrupts current views on extraterritorial jurisdiction to enforce under international law.[9]

To the extent that the computational infrastructure of cyberspace calls into question the epistemological and institutional *pre*suppositions of law and democracy, the design of cyberspace is a public matter that requires democratic participation and should have the full attention of legal experts.[10] This is only possible if legal experts begin to relate to the sciences that contribute to the construction and maintenance of the ICT infrastructure of cyberspace, namely the computer and information sciences, and vice versa. This lecture can be 'read' as a reasoned plea for a dialogue between the sciences that can investigate the architecture of the Rule of Law in cyberspace at the theoretical-normative, empirical and practitioner levels: legal scholarship, computer and information science (including the design of human-machine interfaces)

as well as the cognitive sciences. In this respect we should – as the Flemish would say– 'tune the violins' (i.e. negotiate a shared understanding of what is at stake).

This public lecture consists of four parts. This introduction, ‘Modes of existence’, is followed by ‘Cyberspace does not exist – but it does’ and ‘The cybernetics of the Rule of Law’. After this reconnaissance of the field, I will turn to the real work under the title of 'The Rule of Law after the computational turn'. At this point the reader may object that it is not very useful to start discussing things that do not exist. However, many things that do not exist still exert a great influence. Take Don Quixote and Sancho Panza or Jack and Jill as examples. They may not exist, but we still 'tilt at windmills' and politicians have learned to speak 'Jack and Jill' (i.e. clear, simple language) to get their electorate to 'go along'. How we 'read' reality is largely determined by the metaphors we have available, which in turn determine how we deal with reality.[11] It is good to keep this in mind without walking into the post-modern trap which assumes that we can socially construct reality by telling any story we like about it.[12]

Legal professionals realise better than anyone that the reality we have to deal with is largely based on our shared understanding of that reality. Take for example legal fictions, such as that of the legal person (a ship, a company or a trust).[13] Legal fictions have real and far-reaching consequences, which are based on the legal effect that legislation or case law attributes to specific actions: undergoing punishment, paying compensation, transferring ownership of a house or getting married. The renowned philosophical pragmatist John Dewey once remarked that whereas legal personhood is fictional, in the sense of artificial, and not in the sense of imaginary.[14] An artificial lake, he wrote, is not an imaginary lake. The same applies, for example, to a computer system that behaves as an artificial 'agent' and makes purchases on my behalf. Once the system is (1) capable of autonomously conducting legal transactions, or (2) is held liable for damage incurred to others due to the behaviours of the system (two characteristics of legal entities), things will change for those who employ these 'agents', or do business with them. Legal persons do not exist in the same way as a table or a natural person, but their actions matter. Remember the so-called Thomas theorem: ‘if men define a situation as real, it is real in its consequences’.[15]

Hence, people and things exist in different ways. A stone exists in a different way than a marriage, and Jack and Jill exist in a different way than the office of the Minister of Justice and Security. Nevertheless, this does not prevent us from thinking that people and things exist in a particular way, whereas this is not at all the case. This is the topic of the next part of this lecture.

PART II: CYBERSPACE DOES NOT EXIST – BUT IT DOES

In this section, I briefly consider whether cyberspace as a virtual, non-physical, free space, which we can enter and leave at will, exists at all. The answer is no, and is followed by an exploration of cyberspace as an information-*driven* environment that all of us now inhabit.

CYBER*SPACE* AS A SEPARATE *SPACE*?

The term cyberspace was coined by a science fiction writer. Before cyberspace began to assert its influence, it was already present in the Gibson's novel *Neuromancer* (1984):[16]

> (…) a consensual hallucination experienced daily by billions of legitimate operators, in every nation. A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data.

Cyberspace was discovered before we had empirical proof of its existence. That is nothing very new – the same goes for the gene. In both cases – the gene and cyberspace – the 'theory' or 'the story' preceded the actual discovery or emergence of what is then called the 'gene' or 'cyberspace'.[17]

Cyberspace has long been understood as an unlimited, non-material space, where the law of gravity does not apply and where by default anything and everything is possible.[18] Understood in this way *cyberspace does not exist*: this somewhat exalted notion of cyberspace is an erroneous abstraction of the harsh reality of the hardware, software and protocols that make cyberspace possible, but also constrain it. Think of the data servers that generate the 'cloud', of the software of the tax office that determines whether we qualify for health care allowance, or of the TCP/IP and HTTP and HTML protocols that made the internet and the World Wide Web possible in the first place. We encounter a similar suggestion of an immaterial and immeasurable potential with regard to the emergence of cloud computing, which is often coined as 'virtualisation'. Data management, information management, file sharing, interactive processing of joint work, and even operating systems are supposedly 'virtualised' in cloud computing. Insofar as virtual means the opposite of physical, there is nothing virtual about this state of affairs. Virtualisation refers to the fact that data, databases, platforms, infrastructure and software are no longer present on the user's computer system, but on data servers that provide greater efficiency through economies of scale, while all this is managed by commercial companies. Moreover, those servers – with our data – are increasingly located in countries and jurisdictions where data protection is defined differently than in the European Union, for example in the case of unstable or dictatorial political regimes.[19] Where, in short, our security and our privacy are not necessarily assured. We can conclude that insofar as cyberspace – due to Gibson's metaphorical language – is seen as a non-space or a utopia, it does not exist.

The term cyberspace is derived from the same root as cybernetics, from the Greek word meaning 'to steer' (control) or 'to navigate'.[20] Control can take place in two ways: by grasping an object and forcing it to behave in a certain way, or by giving a subject information that enables it to adjust its own behaviour. Foucault would call the first type of control 'violence' and the second type 'power'.[21] Thaler and Sunstein would call the second type *nudging*, i.e. setting certain defaults that can only be changed after making extra effort.[22] Remote control may involve, for example, building roads in a specific way, which compels road users to behave in a specific way. Just think of the speed bump.[23] It may also involve installing traffic signs with information about the maximum speed. The distinction between coercion on the one hand and an advice or a command on the other is not always obvious. The speed bump can be ignored – at one' s own risk – and therefore falls under the second type of control. The presence of a speed bump provides information to road users. If they are aware of this information, they will probably adjust their behaviour accordingly. The difference with the traffic sign is that the default of the speed bump is much 'tougher' (and more costly if ignored) and that no textual information is provided to back up the default (traffic signs have legal effect, based on the written law; speed bumps do not have legal effect, though they may support the implementation of the law). The default is articulated differently. This is important when it comes to the Rule of Law; I will return to this aspect later on.

Remote control always requires technological mediation: speed bumps, traffic signs, technical protection of data carriers, and paper or online manuals are needed to reach the addressee. Both cyberspace and cybernetics require the combination of information and communication, and both are made possible by the use of technology. Information and communication technology, or ICT, refers to the way in which information transfer and communication are mediated technologically.[24] ICT concerns the infrastructure that in fact determines how we perceive reality beyond direct observation.

The most familiar way to exchange information between human beings is speech. This requires personal proximity, which limits the group of people who can be addressed. It is a non-technological form of communication and control, though not immaterial.[25] The invention of writing was a revolution that enabled the remote control of much larger groups of people. Writing was the first information and communication technology that functioned as an infrastructure. In the course of the last five hundred years, the hand written manuscript has in part been replaced by the infrastructure of the printing press, mass media and the Internet, and currently we are in on the verge of the new era.[26] This concerns the transition to an infrastructure of proactive and – hopefully – interactive computing systems. Awareness of the constitutive influence of the media that enable our perception and cognition has led to a 'mediatic turn' in philosophy and social theory, as with McLuhan, Levy and De Mul. Whereas McLuhan focused primarily on the influence of electricity and automation, Levy and De Mul discussed the transition from the linear, sequential dimension of the book to the parallel, fragmented dimension of hyperlinked text and the corresponding phenomenon of the database. [27]

I focus on a subsequent transformation, which has been coined as a 'computational turn'. The transition to this most recent ICT infrastructure means that our perception and cognition are increasingly mediated by computational technologies. The manipulation of data (the zeros and ones of digital computation)

appears to offer unprecedented possibilities to represent reality in a multiplicity of ways by means of calculation, simulation and prediction. As a result of this development, cyberspace is no longer the safe haven where no one can figure out that you are actually a dog, where you can begin a second life free from all manner of conventions without any of your nearest neighbours knowing about it, or where, through crowd-sourcing, all the knowledge of the world can finally be put together. Even more so than the face-to-face environment, cyberspace is now primarily the space where what you have done is 'known' and what you are going to do is anticipated. Your behaviour is continuously recorded in bits and bytes and is compared with the behaviour of others similar to you, to determine your preferences, anticipate high-risk behaviour, modify prices or predict health problems. And the more cyberspace is capable of predicting the future, the more it appears to create the future. In her book *The Future of Futures*, the Italian philosopher Elena Esposito discussed how the 'present futures' influence the 'future present', focusing on how the automated decision systems of the financial sector both cause and undo their own predictions.[28] The mantra of information-driven coordination in marketing, government and digital forensics gradually leads to all manner of interventions that silently adapt our environment to how advertisers, the tax office or the police 'think' that we will probably behave. Behaviour-driven advertising unobtrusively induces certain behaviours, thanks to a new generation of 'hidden persuaders',[29] that are capable of staying one step ahead of our intentions. In that context, McStay speaks of 'the pre-emption of intent'.[30] The report by the Netherlands Scientific Council for Government policy on 'i-Government' has highlighted the need for networked and enriched data, with the aim of implementing proactive policies based on information-driven risk calculations.[31] The US Department of Defence is conducting the so-called FAST project to investigate the correlation between biometric attributes and future criminal behaviour: Future Attribute Screening Technology. According to a project spokesperson, 'We are running at about 78% accuracy on mal-intent detection, and 80% on deception'.[32] Even if the project has no scientific rigour,[33] insofar as policy makers rely on such inferences, they create their own reality. It is time to expand Robert Merton's Thomas theorem to: 'if machines define a situation as real, then it is real in its consequences'.

As stated above, the linguistic root of cyberspace refers to 'steering' or control. Cybernetics, the science of remote control of human behaviour through technology, has much in common with cyberspace. The field of cybernetics includes not only management-like studies (how can we compel or entice people to exhibit productive behaviour), but also robotics and artificial intelligence. In the 1990s a new technological vision emerged at the interface of cyberspace and cybernetics, called ubiquitous computing, Ambient Intelligence or the Internet of Things.[34] As a result, cyberspace overflowed its banks: by placing RFID chips and sensor technology in every nook and cranny of our physical environment, we can finally take 'the offline world online', as formulated by the International Telecommunications Union. Through the expanding proliferation of Apps, the smartphone effectively connects the online world with the local physical world; for example, consider augmented reality and location-based services. This blurs the distinction between our online and offline environments, demonstrating how cyberspace has passed the stage of a free-floating, virtual non-space. Cyberspace is '*everyware*':[35] it is our information-driven environment, mediated by the artificial intelligence of a growing number of computational techniques.

Conclusion: cyberspace as a hallucination, as disembodied space, as *res cogitans*, as 'free-floating intelligence' independent of human activity and techno-logical embodiment, does not exist. On the one hand this is the case because cyberspace was always already limited by the gravitational forces of the socio-technical architecture that made it possible. On the other hand this is the case because cyberspace has invaded the offline world. Cyberspace does exist, nevertheless, as a field of possibilities conditioned by a highly dynamic set of hardware, software and standardised protocols. As long as those possibilities are not restructured into a golden cage of pre-empted consumer choice, or immunized by increasing government spying, cyberspace provides space to take risks (entrepreneurship), experiment (innovation) and play (both *play* and *game*). But that cannot be taken for granted. To prevent commercial interests from exploiting us as a 'cognitive resource' and to prevent a security-oriented government from *coercing* us into compliance, cyberspace should be engineered and designed in ways that increase our scope for action, instead of decreasing it.[36] This cannot be achieved by merely adding more written law.

PART III: THE CYBERNETICS OF THE RULE OF LAW

In this section I will examine how the law guides and directs people in a constitutional democracy and briefly explain how that particular mode of 'control' is contingent upon the technological infrastructure of the printing press.

THE CYBERNETICS OF THE STATE AND THE RULE OF LAW

The continental traditions of the *Etat de Droit* and the *Rechtsstaat,* and the Anglo-American tradition of the Rule of Law are historical artefacts. They stand for an extraordinarily productive legal and political fiction. In this lecture I will refer to them under the heading of 'the Rule of Law', taking into account their differential fabrication. In legal and political philosophy there is an acute awareness of the historical roots of the Rule of Law. The Rule of Law is not a natural phenomenon or merely an idea; it does not exist in the same way as a stone or a mathematical formula. The law, the state and the Rule of Law are institutions that depend on complex patterns of interaction, which in turn depend on the institutions which enable and constrain them. There is nothing new in reminding us of the artificial, constructed nature of the Rule of Law.

I would, however, like to go one step further and argue that the Rule of Law is also the product of a specific ICT infrastructure: the printing press. This is not often discussed and requires further explanation. In their analysis of legal institutions, neither sociology nor philosophy of law have paid serious attention to the constitutive and regulative role of technology.[37] Technology, in particular information and communication technology, is not just a means to an end. It determines not only what goals can be achieved, or how quickly and to what extent they can be achieved, but also affects the limits of our perception and cognition, thus constraining as well as extending our identity as an individual, as a person and as a society. If it is relatively easy to become acquainted with entirely different ways of living together, we will develop a different type of personality and a different kind of society than when we are only confronted with our own microenvironment, for example, our village or our personalised online environment.[38] The latter can lead to the narrowing of our consciousness, for example because search engines, advertising and advertorials provide us only with information that matches our statistically derived preferences.

Further study of the history of the printing press and the impact of its proliferation at the end of the Middle Ages in Europe has shown that the modern state depends in many ways on the availability of the printed word.[39] *First,* it was precisely this technology that made *remote control* possible: for the first time, a class of officials could be controlled from a central point with reasonably detailed, uniform regulations. *Second,* the abundance of printed texts called for *systematisation* in order to see the forest for the trees. The major codification processes in private law and criminal law testify to this, as did the rise of judicial doctrine as a source of law. *Third,* from the beginning of modernity (16^{th}-17^{th} century), with the rise of private libraries, we see the gradual disappearance of the *master-apprentice relationship*. No longer dependent on the master, students could now easily read not only the primary texts, but also all of the secondary literature. Very different types of texts arose:

pamphlets, newspapers and periodicals. *Fourth,* this led to the emergence of the typically Western practice of critical thinking.[40] Challenged by the ongoing confrontation with conflicting insights, readers and writers began *to relate critically to their own insights*. The book became food for thought, if only because there were so many books: additional relevant knowledge was always available, generating alternative insights. Modern science is exemplary for this approach: a hypothesis is adequate *only* if it is (a) falsifiable, but only *as long as* (b) it has not been falsified. Scientific knowledge is tentative by definition. *Fifth*, the spread of the printing press led to the emergence of a class of writers and scholars who, through their study of the expanding number of texts, could provide perspective and coherence. *This class formed a type of buffer between the sovereign and his subjects.* Because this literate intermediate layer often acquired an effective monopoly on the interpretation of the texts produced by the legislative authority, it was exactly here – often after a long struggle – that an independent judiciary emerged, a judiciary which no longer viewed itself as the voice of the monarch, but claimed to be the voice of law itself.[41]

As a result, interpretation of written legal norms in light of the alleged facts, and qualification of the facts in light of the relevant legal norms, became a crucial aspect of law and of the Rule of Law.[42] The suspending of legal judgement in order to take the time to match fact and norm in a manner that ensured the sustainability of the legal system, are affordances of the proliferation of written text. The realisation that precisely the need for legal certainty requires the court to engage in interpretation, prevented a unilateral determination of 'truth' in law. For this reason, the legislator no longer held a monopoly on the meaning of enacted law; instead, it had to share this monopoly with the courts. The ensuing precarious balance of power has helped to ensure that both state powers contribute to the instrumental and protective functions of law.

THE DOUBLE INSTRUMENTALITY OF THE RULE OF LAW

In my discussion of cyberspace, I made a link with cybernetics and suggested that written law has been, for many years, the most effective way to control, guide or direct people from a distance. As stated previously, you can ‘control’ people by coercing them physically, or by giving them information so they can modify their actions. In the first case I indicated that this concerns the actual manipulation of people as *objects*, while in the second case it concerns holding people to account as *subjects*. However, when people are given information that is not articulated in language (the speed bump or technical protection of software), this easily leads to modifications of behaviour without their conscious awareness. This can be useful, but it can also lead to a form of manipulation that is more subtle than physical coercion, and in the case of behavioural advertising or Ambient Intelligence, this actually amounts to the soft despotism of a smart environment. Such manipulation is perhaps like enlightened despotism, but despotism nevertheless.

In the context of the cybernetics of law, we should distinguish between a public administration perspective, a social science perspective and a legal perspective. Public administrators often tend to view citizens as objects that must be 'regulated'. This is related to the social-scientific nature of their discipline and the methodological individualism that reigns supreme there.[43] Both rational choice theory and the now very popular behavioural economic analysis of human behaviour assume that individuals arrive at certain choices based on full or bounded rationality. For example,

regulation is often defined as: 'the intentional activity which seeks to control, order or influence the behaviour of others.'[44]

That is a rather shallow vision of the meaning of law in a constitutional democracy. Law is indeed an instrument of government regulation, but the Rule of Law is supposed to *simultaneously* offer protection against those regulatory authorities. This implies that legal norms are both constitutive and limitative: they create competences and simultaneously constrain them. Particularly in administrative and criminal law, the principle of legality together with the principles of purpose limitation and proportionality ensures that the law is *simultaneously an instrument of control and an instrument of protection*. In this sense, the Rule of Law stands for the double instrumentality of the law. If the law were only an instrument of government regulation its legal character would disappear, leaving us with the administration or discipline of human behavour. 't Hart and Foqué have referred to the latter as instrumentalism,[45] and argued that the one-sided emphasis on the instrumental function of the law is incapable of offering protection against the totalitarian tendencies of governments – even of those with with the best of intentions. At the same time, they have pointed out the weaknesses of the opposite, critical view of law as pure protection. Such a purely critical law is disconnected from the government power it should constrain, while it is precisely the *constitutive function of law* that prevents instrumentality and legal protection from being played out against each other. To the extent that the law constitutes governmental power, it can simultaneously curb that power and bind it to legal conditions. This prevents thinking in terms of a trade-off between aspects such as security and privacy: security must always be pursued in such a way that privacy is affected as little as possible, and if privacy must be impaired for security purposes, a number of effective safeguards should be provided. Moreover, by maintaining our vision of the double instrumentality of law, we become aware of the fact that loss of privacy always entails loss of security. Knowledge is power. An individual who is fully predictable can be fully manipulated. An individual who no longer has any secrets for others is stripped of the creative, dynamic balance between internal and external, which constitutes both the personal autonomy and relational vulnerability of the self.

Article 8 of the European Convention on Human Rights is an excellent example of this double instrumentality. The first clause stipulates that the right to privacy shall be respected, and the second clause states that there shall be no interference by a public authority with the exercise of this right except when this is in accordance with the law, necessary in a democratic society, and proportional to one of the legitimate aims listed in the clause. The interference must have a basis in law and must comply with certain legal norms, such as foreseeability, accessibility and adequate procedural safeguards. Finally, the relationship between the aim that is to be served and the measure that is to be taken must be proportionate in the light of the seriousness of the interference. That means, for example, that a measure that is not effective is unacceptable, because a measure that does not work cannot be necessary. In short, this article establishes the competence to interfere with the right to privacy but in a way that simultaneously constrains this competence.[46]

THE MODE OF EXISTANCE OF THE RULE OF LAW

Conclusion: the Rule of Law cannot be taken for granted. Like every artificial construction, the Rule of Law is in a state of becoming or in a state of decay.[47]

Control from a distance, systemisation of knowledge, the end of the master-apprentice relationship, the emergence of critical reflection and the creation of an independent judiciary have generated major consequences for the mode of existence of law. Maxims such as *litis finiri oportet* (litigation must come to an end) and *res judicata* (the judgement of the highest court is final) point to the increasing importance of legal certainty. In fact, the significance of positive law (the law that applies here and now) is based on this concept. Natural law emphasised justice, but the flood of conflicting insights that became possible with the spread of the printed word ultimately exposed the elusiveness of the notion of justice. Although the law should aim to achieve justice, we will not easily agree on the meaning of justice.[48] Too much text is out there, with too many differing visions defended. In the era of the printing press, natural law does not bring us together, but drives us apart. Precisely for this reason, positive law cuts through these conflicts. It provides an answer to questions about whether and under exactly what conditions a digital signature is valid, whether a specific case of 'hacking' is a criminal offence, whether a telecom provider can be held liable for its users downloading child pornography, and whether advertising networks should be allowed to process our web browsing behaviours. As long as the flood of regulations and court rulings can be systematised, legal code can offer legal certainty in a way that mathematics, science and art cannot, and precisely as a result of this certainty, the law can be a reliable instrument of government policy. However, the question is whether this also applies in the landscape of smart ICT infrastructures. Our concern here is not only legal certainty, but by extension also regards the question of whether the double instrumentality offered by the Rule of Law can be carried through into the era of computational order.

PART IV THE RULE OF LAW AFTER THE COMPUTATIONAL TURN

Cyberspace creates a new environment for the law that entails a new spatiality. The basic structure of this novel spatiality differs fundamentally from that in which the Rule of Law came to be. The Rule of Law is at stake due to three developments: (1) the computational order of cyberspace increasingly determines our perception, our cognition and the decisions that confront us, while its algorithms are invisible, incomprehensible and often secret, (2) the refined knowledge at the aggregate level can make invisible infringements of the rights to privacy, data protection and the right not to be subject to prohibited discrimination; because these infringements are invisible, the right to contest them is also at issue, and (3) the normative implications of the new ICT infrastructure can easily overrule the normative force of applicable legal norms, turning written law into a paper dragon. We must urgently reflect on the extent to which the current articulation of the law in the technology of the printing press (written law) requires complementary articulation into the computational order it aims to regulate. I will return to this in the final section.

THE COGNITIVE ECONOMY OF THE NEW COMPUTATIONAL ORDER

In March 2011 *The Economist* reported on three start-ups that offer rapid advice (within 15 minutes) on consumer credit.[49] They base their decisions on 'mining' databases with consumer information and/or publicly available information on the web:

> Klarna started by looking at conventional credit scores, but it says that the actual behaviour of shoppers has much more 'predictive power', in the words of Sebastian Siemiatkowski, Klarna's chief executive. The company receives a lot of data from online stores, including things like the time of purchase and whether the consumer's name and address were typed or copied in (the latter is more likely to signal fraud). Wonga draws on 'all publicly available data', in the words of Errol Damelin, Wonga's boss, who does not want to be more specific for security reasons. ReadyForZero accesses data on users' credit-card transactions.
>
> [D]ecisions are made very quickly. Klarna and Wonga feed all the data through elaborate algorithms which determine, almost in real time, how likely it is that a user with a certain data profile will default. Consumers who shop online at 3am may find themselves among the 20% of buyers who get rejected by Klarna. Having a mobile phone with a contract helps to get money from Wonga (which says 'no' to 70% of applications). But no single factor is decisive, says Mr Damelin. 'It's about how the data connect to each other.' Klarna's algorithms are regularly updated to reflect new types of behaviour.

If Wonga's or Klarna's algorithms decide that a loan applicant is an excessive credit risk, her application is denied. My concern here is not whether such a decision would be unfair. My point is that credit decisions are increasingly made by computational techniques which are entirely obscure to the client – and possibly to the credit provider as well. The knowledge on which these decisions are based does not involve the *causes* of the expected payment default nor does it provide any *reasons* for

rejecting an application, it merely detects correlations: 'it's about how the data connect to each other'.[50]

As discussed above, the techniques with which these correlations are mined, recorded, sold and applied have become the backbone of cyberspace. In fact cyberspace builds upon the opportunities already described by McLuhan as arising from universal access to electricity and the associated automation. Unlike the rationalisation and mechanisation of the era of the printing press and the steam engine, McLuhan and cyber-philosopher Lévy find that electricity and automation lead to: decentralised distribution, speed and simultaneity across large distances, parallel rather than sequential processing, and integrated rather than mechanical configurations.[51] To this I would add the ability to make automated decisions based on computing technologies, in particular on machine learning, where the basis of the decision is a statistically derived prediction of future behaviour.[52] *Our access to information* in cyberspace is based on such predictive analytics (the algorithms that determine the search results of Google), the types of advertisements and offers that target us (behavioural advertising), the filtering of news (Google News) and of magazine or journal articles (including the science citation index SCI). *Also, the knowledge that companies, research centres and government agencies* use to make their decisions has become more and more deeply involved in the political economy of what is now called Big Data: medical diagnoses and the corresponding treatment plans, insurance premiums, energy usage management, public and private traffic management, border control, access to employment, criminal investigations, sentencing, the granting social welfare benefits and the combating of social security fraud. All of the sciences, including the humanities, are becoming dependent on automated pattern recognition.[53]

The point is not whether this is good or bad, but first of all what are the implications of all this for how we cognize and perceive our world. The shift from causes (explanations) and reasons (understanding) to correlations and other computational relationships is interesting as well as inevitable, given the quantity of data that is permanently mined and given the complexity of the relationships that are at issue in an ICT infrastructure that thrives on interconnectivity.[54] This shift is related to a new cognitive economy, in which the good life may be reserved for those capable of speedily mining the relevant correlations from floods of otherwise meaningless data. The first challenge will be to keep access to those data and their inferences relatively open, preventing their hiding behind the walls of trade secrecy, national security and intellectual property rights. The second challenge lies in the fact that the shift to 'mined' correlations makes it very difficult to judge claims to accuracy, relevance and reliability. Machine learning presumes that a number of assumptions are made, and it is not an easy task to determine how these assumptions affect the output; different algorithms applied to the same data set will result in differential outcomes, and it is not always evident which representation is the correct, the best or the optimal one. Moreover, the feedback loop inherent to machine learning systems leads, under certain conditions, to 'overfitting'. As a result, outliers may become invisible, resulting in an incorrect confirmation of supposedly prevailing patterns.[55] Since these systems co-constitute the fabric of our cognitive economy, it is of great importance that the perception and cognition they generate is tested and contested such that no knowledge monopolies are established – or sustained – which determine how and what we are capable of knowing. As a result, the Rule of Law is both under threat and compelled to take action. It is under threat because the new knowledge asymmetry disturbs the equilibrium associated with universal access to the written

word. It is compelled to take action because the law can contribute to ensuring equal access to how the knowledge on which we nourish is fabricated, thus enabling the accountability, accuracy, relevance and reliability of the associated knowledge claims. Trade secrets, national security and intellectual property must be articulated in such a way that the source code of cyberspace cannot be hidden from the checks and balances of constitutional democracy.

THE RELATIONSHIP TO FUNDAMENTAL RIGHTS

The Rule of Law is linked to the protection of fundamental rights. Historically, fundamental rights were initially invoked against the state, but increasingly they have become enforceable against other powerful players. The nearly permanent and ever more extensive processing of data by the public and private sectors easily results in violations of the fundamental right to privacy (Article 8 European Convention on Human Rights; Article 7, Charter of Fundamental Rights of the European Union) and the right to fair and legitimate processing of personal data (Articles 6 and 7 Data Protection Directive, Article 8 of the above-mentioned Charter). Many debates have seen the light on this topic, also in relation to the issue of transnational jurisdiction and extraterritorial enforcement.[56] These debates remain, however, a polyphonic, if not cacophonous, spectacle.

Anonymisation, often put forward as the prime technical solution for privacy issues, is not a panacea. This is partly because de-anonymisation is becoming both technologically and economically feasible,[57] and partly because privacy infringements are not always related to the processing of personal data, but may be connected with the application of abstract profiles that can have a much more decisive influence on an individual than the fact that his or her personal data are recorded somewhere.[58] At the same time, one of the most crucial fair information principles, the so-called purpose limitation principle, seems to be at odds with everything cyberspace stands for; data collection is interesting because it produces new knowledge, the added value of which will often become apparent only later.[59] The requirement that it must always be clear in advance why data is being processed appears to stem from another era. Discrimination, in the sense of making invisible and refined distinctions, is at the heart of cyberspace: the capacity to quickly and accurately map out relevant differences is the condition of possibility for adaptivity and personalisation. Nothing wrong with that – unless we are unable to foresee how the environment categorises us and which decisions will arise from that categorisation. If we cannot anticipate this, we cannot contest prohibited discrimination, or prevent undesirable exclusion. That is the problem; an adaptive environment is only of interest for us if we can anticipate it sufficiently. Otherwise it becomes an unsafe haven.

The challenge will be to articulate human rights that provide effective protection against infringements enabled by the new infrastructure, such as the fundamental right derived by the German Federal Constitutional Court on the confidentiality and integrity of computer systems.[60] In this decision, the Court formulated a fundamental right that, for the first time, offers protection against the ICT infrastructure itself. This *infra*structure appeared to have characteristics of an *infringement*structure.[61] After the first generation of human rights that aimed to protect *against* the government, the second generation that aimed to protect *against* powerful societal parties, and the third generation that aimed to protect groups and cultures *from* other forces, we now see an emergent fourth generation that should

offer protection *against* the omnipotence of intransparent computer systems. For a number of reasons it is clear that we should be cautious with proposing new fundamental rights or the expansion of the current scope of human rights.[62] The point is, however, that an entire series of fundamental rights is affected by the computational turn in terms of their mode of existence, in particular privacy, data protection, equal treatment and due process. More written law will not be the solution here, though this does not mean that we can skip linguistic articulation altogether.

In the example of Klarna and Wonga, the fundamental right at stake is the right to be informed about the risk profiles on the basis of which credit decisions are being made. In Article 35 of the Personal Data Protection Act (WBP), Dutch law stipulates the following:

> If so requested, the data controller must provide knowledge of the logic involved in any automatic processing of personal data.

This is an elaboration of Article 12 of the Data Protection Directive and is linked to the right to not be subject to automated decisions (Article 15 of the same Directive, Article 42 of the WBP). What could it mean that we have the right to acquire 'knowledge' of the 'logic of processing' of our personal data? Can we use this information to determine the profiles with which we are matched if the profiles are not derived from our personal data, but from large databases in which anonymised data from millions of other users is stored? Can a provider of credit or a credit rating agency refuse to release information about this logic by appealing to trade secrets or intellectual property rights concerning the database and the software that is used (a possibility mentioned in the preamble to the Directive)? But also, can we understand these this logic if it is provided in the form of a series of algorithms on a DVD?

Article 34 of the German Data Protection Act is much more to the point. It establishes that when a 'score' concerning future behaviour is used in decisions about entering into, executing or terminating a contract (Article 28b), the individual concerned is entitled to the following information:

> 1. the probability values calculated or recorded for the first time within the six months preceding the receipt of the information request,
> 2. the types of data used to calculate the probability values, and
> 3. how the probability values are calculated and their significance, with reference to the individual case and in generally understandable terms.
>
> The first sentence shall apply accordingly if the body responsible for the decision
> 1. stores the data used to calculate the probability values without reference to specific persons but creates such a reference when calculating the probability value, or
> 2. uses data recorded by another body.

These provisions solve a whole series of problems: (1) The information obligation also applies if the 'score' is based on anonymised data, (2) the statistical inferences with respect to future behaviour must be provided, as recorded during the last six months (3a) with an understandable explanation of how the inferences are made (no algorithms, therefore no conflict with trade secrets or copyright) and with (4) a reference to the type of data that are used to calculate the score.

Of course, we can expect that Experian or any other major player in this area will proclaim that this type of information is in fact a trade secret or is protected by copyright, for example because it would enable to reverse engineer the copyright protected code.[63] Another issue is whether we can verify that the software actually

operates in the way the data controller says it does; given the complexity and opacity of much software, it is debatable whether such verification is even theoretically possible.

Equally important is whether the users – the inhabitants of cyberspace – can make sense of this kind of information, and whether they will pay any attention to such information. Moreover, if providing this type of information continues to depend on individual users who take the trouble to ask for it, this will do little to improve the situation. The salient point is therefore that most of the rights formulated above require more than merely written rules. To be effective these rules require complementary re-articulation into the ICT infrastructure they aim to protect against.

Realising the Rule of Law in cyberspace thus involves rethinking the mode of existence of the Rule of Law: written law will not always suffice. This entails research into the extent to which, and the conditions under which, legal protection can be incorporated as a default into the architecture of cyberspace, with a particular focus on access to code that implicates human autonomy and on effective intuitive interfaces.

NEW ARTICULATIONS: LEGAL PROTECTION BY DESIGN?

Legal experts believe, with good reason, that legislation should be technology-neutral. Following Chris Reed, this neutrality can be understood in two ways.[64] On the one hand, as a call *not* to attune statutory regulations to a specific technology, because technology should not determine the content of legal norms. On the other hand, as a call *to pay special attention* to the normative force of specific legal rules given the impact of specific technological development on such normative force. In the second case, neutrality requires a careful analysis of how technologies complement, counteract, erode or enhance the operation of legal norms. This analysis is required precisely because the content of legal norms should not depend on side effects of the evolving ICT infrastructure. The first view seems by now rather outdated, given the dilemmas presented by activities such as hacking, online identity fraud and automated online sales.

The second vision can be illustrated with the so-called cookie legislation. Since 2009, the European ePrivacy Directive has obliged Member States to impose an obligation on data controllers to gain prior and well-informed permission for placing cookies on the end-user's system, especially when used for behavioural advertising. To the extent that the intention was to require prior informed consent for tracking and tracing of a user's web browsing habits, this legislation was already outdated when it came into force. Web beacons, flash cookies, browser fingerprints and other techniques also enable such tracking and tracing. What matters is that 'tracking and tracing' the online behaviour of individuals based on inferred profiles can lead to unwanted transparency, putting existing rights to privacy and data protection at risk of becoming ineffective. Therefore, it would have been better to formulate the obligation to acquire prior informed consent in terms of tracking and tracing techniques and technologies, instead of referring to one particular tracing technology.[65]

Even more interesting would be to acknowledge that smart environments are dependent on the possibility of tracking the machine-readable behaviour of users and on the 'searchability' of the data. To the extent we wish to develop smart environments, it is therefor more important to develop intuitive interfaces with which citizens can gain insight into the multiple manners in which they are 'being read' by

their smart environments. This should give them the means to come to grips with potential consequences. Citizens, consumers and users can then assess much more effectively which of their machine-readable behaviours they prefer to perform when 'unplugged' (unobserved, not being spied upon). Privacy fundamentalists (*excusez le mot*) often appear to fall back on the idea of data minimisation as the default for the information society. Although this is an excellent point of departure in a number of cases, its 'blind' application can lead to failure of the information-*driven* society. Unless we reject data-driven infrastructures we must develop smart minimisation, rather than minimal disclosure per se. This should be based on an adequate assessment of the risks of data sharing. This assumes much greater and much more intuitive transparency, than has been available so far. This reminds me of the 'Reveal Codes' feature in WordPerfect, with which you could quickly and easily detect problems in the template of your text, unlike with Microsoft Word, which makes you guess about which automatic mechanisms are trying to anticipate your behaviour. Time has come for the proactive dimension of Microsoft Word to be combined with the transparency of WordPerfect, so that we are no longer part of someone else's feedback loop, and can effectively interact with it ourselves.[66] It is time to invest in apps that enable us - at any time we choose - to see who is observing us from which location, what profiles determine the 'content' we get to see and how data analysis affects the decisions we are subject to. In order to make this possible, the apps could require access to the source code of the service providers. Insofar as our everyday perception and cognition within cyberspace depend on the algorithms that personalise the environment, we – citizens of cyberspace – must negotiate some form of effective access to the source code. Without such transparency the Rule of Law will not thrive. We must gain such acces even if it impinges on trade secrecy, national security or the copyright to the source code. These should all be respected, but not at the cost of the substance of personal freedom.

In closing, this brings me to a more general conclusion, which concerns the technological articulation of modern law. As Lessig wrote:[67]

> the character of an era hangs upon what needs no defence.

The primacy of enacted, written law is directly related to the rise of the printed word. In the era of the printing press, that primacy has come to be taken for granted, as did the related need for judicial interpretation. The balance of powers that has been achieved between legislator, administration and courts, after long struggles on who reigns superior, needs to be reinvented. The technological conditions of possibility have changed. The defaults of cyberspace nudge us in the wrong direction: towards sharing and leaking unlimited amounts of data without an inkling of how our data points match what profiles. These defaults will not changes of themselves. Although cyberspace was once seen as a place where the sun always shines because social control, government inspection and commercial interference are absent, it has now become clear that even an umbrella cannot protect us from a personalised downpour, based on unobtrusive surveillance and refined pattern recognition. Simply referring to the possibility of taking an umbrella no longer suffices. Law and the Rule of Law in cyberspace will, to a certain extent, depend on a new technological articulation of legal protection. Legal experts can build upon the idea of value-sensitive design, a design practice that is affiliated with research into the embodiment of ethical values and norms into technological artefacts.[68] Insofar as the Rule of Law is at stake, however, ethical reflection is pertinent but not sufficient. The law not only offers

protection against undesirable asymmetries of knowledge, but also provides enforcement. Legislators in democracies should consider the design of cyberspace, and the courts should consider its implications. To preserve our relative autonomy,[69] privacy and the capability to participate in public and private versions of the good life, will require that we defend them, or better still, reinvent them at the level of the architecture that should at least afford them.

Notes

· This 'street-art' by Bansky refers to the fact that cyberspace was first mistaken for a place where the sun always shines, because social controle, government inspection and commercial interest were non-existen. By now it should be clear that even with an umbrella cyberspace allows for targeted raining.

[1] See http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz.

[2] See http://europe-v-facebook.org/EN/en.html. Facebook's responses, which I quote later on, are also published on this site.

[3] Irish Data Protection Act 1988 (revised and updated 30th March 2012), art. 4(1)(iv).

[4] Ibid., art. 4(12).

[5] Ch. Ess and R. Hagengruber (eds.) *The Computational Turn: Past, Presents, Futures?* Proceedings International Association for Computer and Philosophy 2011 (Münster: Monsenstein und Vannerdat, 2011). D.M. Berry, *Understanding Digital Humanities: The Computational Turn and New Technology* (London: Palgrave Macmillian, 2011). I. Ayres, *Super crunchers : why thinking-by-numbers is the new way to be smart* (New York: Bantam Books, 2007). M. Hildebrandt, E. De Vries (eds.), *Privacy, Due process and the Computational Turn. Philosophers of law meet philosophers of technology*, in review with Routledge-Cavendish. With contributions by Martijn van Otterlo, Lorenzo Magnani, Ian Kerr, Elena Esposito, Antoinette Rouvroy, Finn Brunton & Helen Nissenbaum, Bert-Jaap Koops, Mireille Hildebrandt, Katja De Vries & Solon Barocas.

[6] D. Ihde, *Ironic Technics* (Automatic Press / VIP, 2008).

[7] M. Kranzberg, "Technology and History: 'Kranzberg's Laws'," *Technology and Culture* 27 (1986): 544-560.

[8] M. McLuhan, *Understanding Media. The Extensions of Man* (Cambridge MA: MIT Press, 1964).

[9] M. Hildebrandt,

[10] W. Bijker, *Democratisering van de Technologische Cultuur* (Maastricht: Rijksuniversiteit Limburg, 1995). A. Meijer, "We moeten vechten voor democratisering van cyberspace," *De Volkskrant*, November 7, 2011.

[11] G. Lakoff and M. Johnson, *Metaphors We Live By*, 2nd ed. (University Of Chicago Press, 2003).

[12] Against such naive social constructivism e.g. B. Latour, *Reassembling the Social. An Introduction to Actor-Network-Theory* (Oxford: Oxford University Press, 2005).

[13] See also T. E. Huff, *The Rise of Early Modern Science. Islam, China, and the West, second edition* (Cambridge UK: Cambridge University Press, 2003), which describes how modern Western science owes its existence to the legal entity of the *universitas*, the legal form from which the universities derive their name. Compare also H. Berman, *Law and Revolution. The Formation of the Western Legal Tradition* (Cambridge Massachusetts and London, England: Harvard University Press, 1983).

[14] J. Dewey, "The Historic Background of Corporate Legal Personality," *The Yale Law Journal* 35, no. 6 (1926): 655-673.

[15] Popularised by philosopher of science R. K. Merton, "The Self-fulfilling Prophecy," *The Antioch Review* 8, no. 2 (1948): 193-210, who borrowed it from W. I. Thomas, D. S. Thomas, *The Child in America* (New York: Knopf, 1928). With this statement, Merton refers to the fact that misrepresentations have real effects once people believes them to be true (the self-fulfilling prophecy). From a constructivist perspective, however, the statement is a truism, which can be better understood in relation to the work of Austin and Searle. Compare J. L. Austin, *How to Do Things with Words* (2nd ed. Harvard University Press, 1975), and J. Searle, *The Construction of Social Reality* (New York: The Free Press, 1995). For the law see N. MacCormick and O. Weinberger, *An Institutional Theory of Law: New Approaches to Legal Positivism* (Dordrecht: Kluwer 1986).

[16] W. Gibson, *Neuromancer* (Ace, 1984). There is some similarity to E. M. Forster's short story 'The Machine Stops' from 1928.

[17] E. Fox Keller, *The Century of the Gene* (Cambridge, Massachusetts: Harvard University Press, 2000). The internet, the collaboration of various computer networks based on the TCP/IP protocol, was under construction when Gibson published his novel. The internet was the 'condition of possibility' of the World Wide Web, which emerged in the early 90s as a result of the HTTP and HTML protocols that enabled the use of hyperlinks.

[18] Compare J. P. Barlow, *A Declaration of the Independence of Cyberspace* (Davos, Switzerland, 1996). Compare J. E. Cohen's criticism of the idea of cyberspace as a separate space, "Cyberspace As/And Space," *Columbia Law Review* 107 (2007): 210-256.

[19] Though the EU also defines the US as a jurisdiction without adequate data protection. See e.g. Marc Rotenberg and David Jacobs, "Privacy, Security, and Human Dignity in the Digital Age: Updating the

Law of Information Privacy: the New Framework of the European Union," Harvard Journal of Law & Public Policy 36 (n.d.): 637-641.

[20] N. Wiener, *Cybernetics: or the Control and Communication in the Animal and the Machine* (2nd ed. MIT Press, 1965).

[21] M. Foucault, "The Subject and Power," *Critical Inquiry* 8, no. 4 (July 1, 1982), p. 789. Foucault sees power at that moment as a '*conduit des conduites*'; regarding privacy in this respect, see: P. De Hert, S. Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power," in: E. Claes, A. Duff, and S. Gutwirth (eds.) *Privacy and the Criminal Law* (Antwerpen Oxford: Intersentia, 2006), p. 73.

[22] R. H. Thaler and C. R. Sunstein, *Nudge : improving decisions about health, wealth, and happiness* (New Haven: Yale University Press, 2008).

[23] Or building viaducts in such a way that the bus which carries poor, lower-class passengers cannot pass. See L. Winner, *The whale and the reactor: a search for limits in an age of high technology* (Chicago: University of Chicago Press, 1986).

[24] Here I define technology as an instrument or method with a material component. See Don Ihde, 'Philosophy of technology: an introduction', vol. 1, *Paragon issues in philosophy* (New York: Paragon House, 1993), p. 47-48 and J. Sawday, *Engines of the imagination: Renaissance culture and the rise of the machine* (Taylor & Francis, 2007), p. 2. Both authors emphasise the materiality of technology. The term 'technique' is also used, which I define as 'method' or 'way of doing'.Regarding the 'mediatic turn' in philosophy: J. De Mul, "Wittgenstein 2.0: Philosophical Reading and Writing after the Mediatic Turn," in: A. Pichler, H. Hrachovec (eds.) *Wittgenstein and the Philosophy of Information: Proceedings of the 30th International Ludwig Wittgenstein-Symposium in Kirchberg, 2007*, (Ontos Verlag, 2008), 153-179.

[25] As Stiegler explains in, "Die Aufklaerung in the Age of Philosophical Engineering," translated by Daniel Ross, in *The Value of Personal Data. Digital Enlightenment Forum Yearbook 2013*, eds. Mireille Hildebrandt, Kieron O'Hara, and Michael Waidner (Amsterdam: IOS Press, 2013), after the keynote given at the W3C Conference in 2012, available at http://www2012.wwwconference.org/documents/Stiegler-www2012-keynote.pdf.

[26] Despite Morozov's delicious bashing of media study pundits (E. Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (New York: Public Affairs, 2013), I believe that we have a lot to learn from philosophers of technology. Notably those who avoid the traps of determinism, techno-pessimism or techno-optimism: D. Ihde, *Technology and the Lifeworld : from Garden to Earth* (Bloomington: Indiana University Press, 1990).

[27] McLuhan, *Understanding Media. The Extensions of Man*. P. Lévy, *Les technologies de l'intelligence. L'avenir de la pensée à l'ère informatique* (Paris: La Découverte, 1990). J. De Mul, *Database Delirium* (Amsterdam: Bert Bakker, 2006).

[28] E. Esposito, *The Future of Futures: The Time of Money in Financing and Society* (Edward Elgar Publishing, 2011).

[29] Cf. V. Packard, *The Hidden Persuaders* (Pocket, 1984).

[30] A. McStay, *The mood of information : a critique of online behavioural advertising* (New York : Continuum, 2011), p. 3.

[31] Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid* Rapport nr. 86, (WRR, 2011)

[32] See the IATA website http://www.iata.org/whatwedo/safety_security/security/Pages/checkpoint-future.aspx.

[33] S. Weinberger, "Terrorist 'pre-crime' detector field tested in United States. Screening system aims to pinpoint passengers with malicious intentions," *Nature* (May 27, 2011), http://www.nature.com/news/2011/110527/full/news.2011.323.html.

[34] M. Weiser, "The computer for the 21st century," *Scientific American* 265, no. 3 (1991): 94-104. ITU, *The Internet of Things* (Geneva: International Telecommunications Union (ITU), 2005). ISTAG, *Scenarios for Ambient Intelligence in 2010* (Information Society Technology Advisory Group, 2001). E. Aarts and S. Marzano, *The New Everyday. Views on Ambient Intelligence* (Rotterdam: 010, 2003).

[35] A. Greenfield, *Everyware. The dawning age of ubiquitous computing* (Berkeley: New Riders, 2006).

[36] The canonical texts in this field include: L. Lessig, *Code Version 2.0* (New York: Basic Books, 2006). L. Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (Vintage, 2002).R. Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford: Oxford University Press, 2008). In Dutch: R. Leenes, Harde lessen. Apologie van Technologie als Reguleringsinstrument (Tilburg: Universiteit van Tilburg, 2010).

[37] 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): 169-183.
[38] C. Sunstein, *Republic.com* (Princeton and Oxford: Princeton University Press, 2001). E. Pariser, *The Filter Bubble. What The Internet Is Hiding From You* (Penguin Viking, 2011). T.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 (2003 2002): 17-47. M. Hildebrandt, Serge Gutwirth, *Profiling the European Citizen. Cross-disciplinary Perspectives* (Dordrecht: Springer, 2008).
[39] E. Eisenstein, *The Printing Revolution in Early Modern Europe* (Cambridge New York: Cambridge University Press, 2005). W. Ong, *Orality and Literacy: The Technologizing of the Word* (London/New York: Methuen, 1982). W. Chappell, R. Bringhurst, *A Short History of the Printed Word* (Vancouver: Hartley & Marks, 1999). A. Reinhardt, "Bookreview of: Gutenberg in Shanghai: Chinese Print Capitalism, 1876-1937. By Christopher A. Reed. Vancouver: University of British Columbia Press, 2004," *Technology and Culture* 46, no. 2 (2005): 411-413. J. Habermas, *Strukturwandel der Offentlichkeit. Untersuchungen zu einer Kategorie der burgerlichen Gesellschaft* (Frankfurt am Main: Suhrkamp, 1962).
[40] N. Carr, *The Shallows: What the Internet is Doing to Our Brains* (New York: W.W. Norton, 2010). M. Wolf, *Proust and the Squid: The Story and Science of the Reading Brain* (Icon Books Ltd, 2008).
[41] P. Koschaker, *Europa und das römische Recht*, vol. 4 (München: C. H. Beck'sche Verlagsbuchhandlung, 1966). H. Patrick Glenn, *Legal Traditions of the World* (Oxford: Oxford University Press, 2007).
[42] On the role of interpretation in the era of the printing press, Lévy, *Les technologies de l'intelligence. L'avenir de la pensée à l'ère informatique*. On hesitancy as a characteristic of judicial labour, B. Latour, *La fabrique du droit. Une ethnographie du Conseil d'État* (Paris: La Découverte, 2004).
[43] See for example M. Bovens, *De digitale rechtsstaat. Beschouwingen over informatiemaatschappij en rechtsstaat*, inaugural address Utrecht 1998 (Alphen aan den Rijn: Samsom, 1999). Bovens refers to the information society, which he defines in terms of deterritorialisation, turbulence, horizontalisation and dematerialisation. What I am concerned with here is the information-*driven* society, or cyberspace.
[44] See the often-quoted definition of Julia Black: 'the intentional activity of attempting to control, order or influence the behaviour of others', for example in: Ch. Parker et al. (eds.) *Regulating law* (Oxford New York: Oxford University Press, 2004). Moreover, Black herself is acutely aware of the problematic aspects of the regulatory paradigm, see J. Black, "Critical Reflections on Regulation," *Australian Journal of Legal Philosophy* 27 (2002).
[45] R. Foqué and A.C. 't Hart, *Instrumentaliteit en rechtsbescherming* (Arnhem Antwerpen: Gouda Quint Kluwer Rechtswetenschappen, 1990).
[46] Compare for example S. Sottiaux, *Terrorism and the Limitation of Rights. The ECHR and the US Constitution* (Oxford: Oxford University Press, 2008). Chapter 6.
[47] According to the second law of thermodynamics this applies to everything: without the input of energy, everything decays into entropy. In that sense, there is only becoming and no being – a sentence that would contradict itself if the word 'is' were to be misunderstood. Prigogine, I., I. Stengers, *Order out of Chaos.* (New York: Bantam Books, 1984). A.N. Whitehead, *Process and Reality* (New York: Macmillan, 1929).
[48] See especially Feuerbach, compare G. Radbruch, *Feuerbach; bearbeitet von Gerhard Haney*, ed. Arthur Kaufmann, Gesamtausgabe Gustav Radbruch (Heidelberg: Müller, 1997).
[49] "Data-driven finance. Go figure. A new class of internet start-ups is trying to turn data into money," *The Economist* March 17th (2011).
[50] In the Netherlands, Experian, which calls itself 'the global leader in the provision of information, analysis and marketing services to businesses and consumers,' offers a Credit Check: 'a secure online product that, based on reliable data, allows you to quickly decide whether or not to accept a customer. You can search by name and/or address and the data are immediately available. You can also link the Credit Check to your own systems so you can make sound decisions automatically. The Credit Check is used primarily in the telecommunications, utilities, cable, retail and real estate sectors.' See: http://www.experian.nl/kredietrisico-management/informatie-en-scoringsmethoden-credit-check.html, visited most recently on 2 November 2011.
[51] McLuhan, *Understanding Media. The Extensions of Man*. Lévy, *Les technologies de l'intelligence. L'avenir de la pensée à l'ère informatique*.
[52] T.M. Mitchell, *The Discipline of Machine Learning* (Carnegie Mellon University, School of Computer Science, 2006), available at http://www-cgi.cs.cmu.edu/~tom/pubs/MachineLearningTR.pdf.

[53] W.H. Dutton and P.W. Jeffreys, *World Wide Research* (MIT Press, 2010). Berry, *Understanding Digital Humanities: The Computational Turn and New Technology*. V. Mayer-Schönberger, K. Cukier, *Big Data: a Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013).

[54] See also C. Anderson, "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete," *Wired Magazine* 16, no. 7 (2008). His position is somewhat 'over the top', but is interesting from an epistemological perspective. In other work I have stated that Peirce's pragmatic maxim can sometimes be highly relevant to a proper understanding of the type of knowledge that can be derived based on machine learning: M. Hildebrandt, "Who is profiling who? Invisible visibility," in: S. Gutwirth et al. (eds.) *Reinventing Data Protection?* ed. (Dordrecht: Springer, 2009), 241.

[55] T. Dietterich, "Overfitting and undercomputing in machine learning," *ACM Comput. Surv.* 27, no. 3 (September 1995): 326–327. C. Ciborra, "Digital Technologies and the Duality of Risk", CARR Discussion Papers, DP27. (Centre for Analysis of Risk and Regulation, LSE, London UK, 2004). B.E. Harcourt, *Against prediction : profiling, policing, and punishing in an actuarial age* (Chicago: University of Chicago Press, 2007).

[56] P. De Hert, S Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action," in S. Gutwirth et al. (eds.) *Reinventing data protection?* (Dordrecht: Springer, 2009), p. 3-44. Ch. Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)," *International Journal of Law and Information Technology* 18, no. 2 (June 20, 2010): 176 -193. C. Cuijpers and B.-J. Koops, "How Fragmentation in European Law Undermines Consumer Protection: The Case of Location-Based Services," *SSRN eLibrary* (n.d.), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1645524.

[57] P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57 (2010): 1701-1777.

[58] A. Vedder, "KDD: The challenge to individualism," *Ethics and Information Technology* 1 (1999): 275-281. B. Custers, The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology (Nijmegen: Wolf Legal Publishers, 2004). M. Hildebrandt, "Profiling and the identity of the European citizen," in: M. Hildebrandt, S. Gutwirth (eds.) *Profiling the European citizen. Cross-discplinary perspectives* (Dordrecht: Springer, 2008).

[59] B. Massiello, A. Whitten, "Engineering Privacy in a Age of Information Abundance," in *Intelligent Information Privacy Management* (AAAI, 2010), 119-124.

[60] BVerfG, 1 BvR 370/07 of 27.2.2008. I use the term 'on account of' here to avoid the discussion on the question of whether an infrastructure can violate rights.

[61] Also consider the emergence of *deep packet inspection* (DPI), compare P. Ohm, "The Rise and Fall of Invasive ISP Surveillance," *University of Illinois Law Review*, no. 5 (2009): 1417-1496. M Hildebrandt, "Who needs stories if you can get the data? ISPs in the era of big number crunching", *Philosophy and Technology* (2011).

[62] See also J. Gerards, *Het prisma van de grondrechten*, inaugural lecture Nijmegen 2011. B.-J. Koops, "Digitale grondrechten en de Staatscommissie: Op zoek naar de kern", *Tijdschrift voor constitutioneel recht* 2, nr. 2 (2011): 168-185.

[63] See also the preliminary questions in the case of SAs v World Programming before the European Court of Justice in Luxembourg C-406/10.

[64] Ch. Reed, "Taking Sides on Technology Neutrality," *SCRIPT-ed* 4, no. 3 (2007): 263-284. L. Lessig, *Code Version 2.0* (New York: Basic Books, 2006), especially Chapter 9 'Translation'.

[65] In fact, the Art. 29 Working Party has clarified that the relevant legislation applies also to similar tracking techniques. See Opinion 04/2012 on the Cookie Consent Exemption, WP194, at 2: 'Article 5.3 impacts on the usage of cookies but the term should not be regarded as excluding similar technologies'.

[66] See E. Aarts, F. Grotenhuis, "Ambient Intelligence 2.0: Towards Synergetic Prosperity," in: Manfred Tscheligi et al. (eds.) *AmI 2009* (Berlin Heidelberg: Springer, 2009), 1-13. These authors appear to be convinced of this already. The Reveal Codes feature of WordPerfect was a smart interface. The importance and influence of intuitive interfaces (such as touch screen technology and Microsoft's Kinect, but also neuromarketing) require special attention. Regarding the study of Human Machine Interaction, see: J.M. Carroll, "Conceptualizing a possible discipline of human–computer interaction", *Interacting with Computers* (22) 2010-1: p. 3-12.

[67] Lawrence Lessig, The Future of Ideas: The Fate of the Commons in a Connected World (Vintage, 2002), p. 5.

[68] P.-P. Verbeek, "Materializing Morality. Design Ethics and Technological Mediation," Science Technology & Human Values 31, no. 3 (2006): 361-380. M. Flanagan, D. Howe, H. Nissenbaum,

"Values in Design: Theory and Practice", in: J. Van den Hoven, J. Weckert (eds.) Information Technology and Moral Philosophy (Cambridge: Cambridge University Press, 2007). E. Dommering and L. Asscher, Coding Regulation (The Hague: T.M.C. Asser Press, 2006). 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): 428-460. M Hildebrandt, "Legal Protection by Design: Objections and Refutations", Legisprudence (2011): 223-248.

[69] M. Hildebrandt, "Autonomic and autonomous 'thinking': preconditions for criminal accountability," in: M. Hildebrandt, A. Rouvroy, *Law, Human Agency and Autonomic Computing. The Philosophy of Law meets the Philosophy of Technology* (Abingdon: Routledge, 2011).