Onlife, The Public(s) and Legal Protection by Design

Mireille Hildebrandt
C.4. Technology Neutrality and Legal Protection by Design  
C.5. The proposed Data Protection Regulation  
Bibliography
A. ONLINE after the computational turn?

A.1. Computational turn

In my inaugural lecture I have reiterated the notion of a computational turn, referring to the novel layers of software that have nested themselves between us and reality. These layers of decisional algorithmic adaptations increasingly co-constitute our lifeworld, determine what we get to see (search engines; behavioural advertising), how we are treated (insurance, employment, education, medical treatment), what we know (the life sciences, the digital humanities, expert systems in a variety of professions) and how we manage our risks (safety, security, aviation, critical infrastructure, smart grids). So far, this computational turn has been applauded, taken for granted or rejected, but little attention has been paid to the far-reaching implications for our perception and cognition, for the rewoven fabric on which our living-together hinges (though there is a first attempt in Ess and Hagen-gruber 2011, and more elaboration in Berry 2012). The network effects of ubiquitous digitization have been described extensively (Castells 2011; Van Dijk 2006), though many authors present this as a matter of ‘the social’, neglecting the extent to which the disruptions of networked, mobile, global digital technologies are indeed ‘affordances’ of the socio-material assemblages of ‘the digital’. Reducing these effects to ‘the social’ does not help, because this leaves the constitutive and regulative workings of these technologies under the radar. Moreover, we need to distinguish between digitization per se and computational techniques such as machine learning that enable adaptive and proactive computing and thereby present us with an entirely novel – smart – environment.

A.2. Smart environments

I believe that whereas such smart environments have long remained a technological fantasy, they are now with us, around us, inside us. They anticipate our future behaviours and adapt their own behaviours to accommodate our inferred preferences – at least insofar as this fits the objectives of whoever is paying for them (commercial enterprise, government). They provide us with a ubiquitous artificial intelligence that uproots the common sense of our Enlightenment heritage that matter is passive and mind active. Matter is developing into mind, becoming context-sensitive, capable of learning on the basis of feedback mechanisms, reconfiguring its own programs to improve its performance, developing ‘a mind of its own’, based on second-order beliefs and preferences. This means nothing less than the emergence of environments that have agent-like characteristics: they are viable, engines of abduction, and adaptable (Bourgine and Varela 1992); they are context-sensitive, responsive, and capable of sustaining their identity by reconfiguring the rules that regulate their behaviours (Floridi and Sanders 2004). We should note, however, that ‘they’ do not need to be consciously aware of any of this, let alone be self-conscious. Also, let’s acknowledge that we are not talking about what Clark (2003) termed ‘skinbags’: neatly demarcated entities that contain their mind within their outer membranes, surface or skin. The intelligence
that emerges from the computational layers engineered to serve specific purposes - while thriving on the added value created by unexpected function creep – this emergent intelligence derives from polymorphous, mobile computing systems, not from stand-alone devices such as those fantasised in the context of humanoid robotics.

A.3. What’s new here?

In what sense is this a novel situation? Where lies the continuity with preceding information and communication technologies? In his magnificent *Les technologies de l’intelligence* Pierre Lévy (1990) discusses the transitions from orality to script, printing press and mass media towards digitisation and the internet. Summing up, Lévy suggests we are in a transition from a linear sense of time to segments and points; from accumulation to instant access; from delay and duration to real time and immediacy; from universalisation to contextualisation; from theory to modelling; from interpretation to simulation; from semantics to syntaxis; from truth to effectiveness; from semantics to pragmatics; from stability to change. Interestingly, his focus is on ubiquitous computing and highlights the impact of the hyperlink, but hardly engages with the computational intelligence described above. Core to the novel, ambient intelligence, is the fact of being anticipated by invisible complex computing systems (Stiegler 2012). Their capacity to generate data derivatives (Amoore 2011) and to pre-empt our intentions on the basis of personalised inferences creates what Catherine Dwyer (2009) has called ‘the inference problem’. The thingness of our artificial environment seems to turn into a kind of subjectivity. In other work I have suggested that social science has long since recognized the productive nature of the inference problem that nourishes relationships between people (2011a). Parsons and Luhmann spoke of the so-called double contingency that determines the fundamental uncertainty of human interaction (Vanderstraeten 2007). Since I can never be sure how you will read my words or my actions, I try to infer what you will infer from my behaviours; the same goes for you. We are forever guessing each other’s interpretations. Zizek (1991) has qualified the potentially productive nature of this double and mutual anticipation by suggesting that ‘communication is a successful misunderstanding’. What is new here is that the computational layer that mediates our access to knowledge and information is anticipating us, creating a single contingency: whereas it has access to the data to make its inferences, we have no such access and no way of guessing how we are being ‘read’ by our novel smart environments.

A.4. Which are the challenges?

If going ONLIFE refers to immersing ourselves in the novel environments that depend on and nourish the computational layers discussed above, then going ONLIFE will require new skills, different capacities and other capabilities. To prevent becoming merely the cognitive resource for these environments we must figure out how they are anticipating us. We must develop ways to extend the singly contingency to a renewed double contingency. How to read
in what ways we are being read? How to guess the manner in which we are being categorized, pre-empted, foreseen? How to keep surprising our environments, how to move from proaction to interaction? In other work I have suggested that we need to probe at least two tracks: first, to develop human machine interfaces that give us unobtrusive intuitive access to how we are being profiled, and, second, a new hermeneutics that allows us to trace at the technical level how the algorithms can be ‘read’ and contested. For now, the point I would like to make is that the implications of going ONLIFE cannot be reduced to privacy and data protection. I hope that the previous analysis demonstrates a far more extensive impact that cannot be understood solely in terms of the wish to hide one’s personal data. It requires more than hiding one’s data; indeed it challenges us to engage with our environments as if we are taking ‘the intentional stance’ with them (Dennett 2009).

B. Publics and their problems in smart environments

B.1. Smart environments and the public sphere

Above I have tried to flesh out in what sense smart environments present us with a novel situation. My conclusion was that the computational layers that mediate our perception and knowledge of the world are generating an environment that simulates agency. Whereas the International Telecommunications Union spoke of the Internet of Things as ‘the offline world going online’, in some sense the plethora of autonomic decision systems are turning our inanimate environment ‘ONLIFE’. Since we had decided to more specifically look into what this means for the public sphere, or for the traditional private/public divide in itself, I will now try to engage with the notion of the public sphere and see whether and how smart environments generate a kind of ‘natality’ here. A novelty, a beginning, an empty space to experiment – with as yet unknown affordances.

B.2. Public private social: Performance, exposure, opacity

Enough has been written about the shrinking of the private, the blurring of the public/private divide and e.g. the loss of privacy in the public (Nissenbaum 1997). All this has been attributed to either the lure of self-publication in web 2.0, or to the secretive trading with and spying on our behavioural data in the course of pervasive computing (Hildebrandt 2012).

Maybe we should return to Arendt (1958), when she spoke of the private as a sphere of necessity (the household), the public as the space for freedom (political action) and ‘the social’ as the emergence of mass society (bureaucracy, individual self-interest and conformity). Her understanding of ‘the social’ or what she calls ‘society’ is not altogether positive, to put it mildly. Is the rise of web 2.0 antithetical to ‘the social’, because it concerns communication of one-2-one, one-2-many as well as many-2-many, rather than many-
2—one? Or does the processing of Big Data present us with ‘the social’ come true, where it is constituted by machine readable bits and pieces that allow for the ultimate version of what Heidegger (1996) called ‘das rechnende Denken’ (calculative thinking)? I am not sure, and I believe the jury is still out. The answer will be empirical and will depend on how ‘the social’ will evolve in smart environments.

I do think that Arendt’s understanding of the private and the public might save us from dichotomous thinking, as well as from the glorification of ‘private life’ as a sphere of uncontroversial freedom. Though we must also come to terms with the fact that her glorification of the public sphere has little connection with present day politics, which rather falls within the scope of her depiction of ‘the social’. At the same time, also, we must note that her glorification of politics as a ‘theatre of debate’ [instead of the realm of household economics] is rooted in an appreciation of privacy as ‘some darker ground which must remain hidden if it is not to lose its depth in a very real, non-subjective sense’ (Arendt 1958). To speak and act ‘in public’ one must leave the security of one’s home. But to distinguish oneself and to take the risk of being refuted, requires courage, daring and a place to hide. To recuperate from the tyranny of public opinion (Mill 1859) we need a measure of opacity to re-constitute the self, far from the social pressures that could turn us into obedient self-disciplined subjects (Hutton et al. 1988). In fact I would agree with Butler (2005), where she underscores the constitutive opacity of the self, that invites reiterant attempts to invent a coherent narrative of who we are, but at the same time escapes all narrative since the emergence of our self is hidden in our own prehistory (the infancy before we acquired language).

My question concerning the public in smart environments would thus be: how to design our ONLIFE in a way that affords a sustainable public performance, an empowering opacity of the self and a range of exposures that incorporates the need for self-expression, identity performance as well as the generosity of forgetfulness, erasure and the chance to reinvent oneself?

### B.3. Public Performance in the ONLIFE everyware

Maybe ONLIFE has two dimensions, as suggested above. The first concerns self-publication or reputation management. It is a type of social networking (Facebook, Twitter, Foursquare, Instagram, Youtube, Training Intelligence Programs, Enhanced Reality), i.e. pervasive sharing of self-images, brief texts, photo’s, video’s, location, ‘likes’, ‘dislikes’, sport’s performance, health status, professional reputation. The second concerns the ubiquitous measurement, calculation and manipulation of the data that leak from everyday behaviours, which are used to predict, pre-empt and thus manage future states of mind, choices and decisions, i.e. behavioural advertising, location based services, fraud detection, actuarial calculations, remote healthcare, neuromarketing, criminal profiling,
Both seem to draw individual ‘users’ into Arendt’s ‘the social’: ‘users’ have become what she calls ‘a society’. An assembly of individuals that are managing their reputation, while also being managed as a resource for government and the industry. I would add that the computational infrastructure is in fact ‘using’ the traces that ‘users’ leave as its cognitive resource.

What affordances must ONLIFE have to develop a shared, agonistically organised public space that allows a plurality of ‘users’ to develop a voice, to partake in democratic decision-making and to hold each other to account. While at the same time providing them with effective means to withdraw, to unplug, to delete and start over.

- How to protect ‘users’ against invisible manipulation (because of the hidden complexity), unfair exclusion (because of the lack of transparency that disables contestation), and undesirable exposure (because of the ubiquitous pressure to ‘post’ an update of one’s where/what/who-abouts?
- How to empower ONLIFE inhabitants in a way that enables them to challenge the design of their world? Is this about renegotiating the social contract? Or is it about construction work: how to build an ONLIFE world that is not a global village, nor a walled garden, but an extended urbanity?
- How does this connect to the dimension of agency that is emerging within the ONLIFE experience; how could inhabitants or visitors of the ONLIFE learn to guess how they are being anticipated?

B.4. A plurality of publics, a choice of exposure, a place to hide

In 1927 Dewey wrote The public and its problems. The book is an extended reply to Lippman’s (1997) analysis of democratic government in the age of mass media, high tech instrumentation and societal complexity. I find his analysis and his normative position on democratic practice highly relevant for our enterprise. As Marres (2005) has demonstrated Dewey agrees with Lippman’s diagnosis, but not with his cure. Whereas Lippman believes the only solution is technocratic government, Dewey argues for a new understanding of democracy. For a start, he reminds us that representative democracy (voting) is a matter of delegation, relieving people from the burden of governing themselves. Second, he believes that once people discover that their delegates are not doing a good job with regard to a specific issue, they will seek out their fellows and form a public around this issue. Interestingly, the formation of publics and issues is a matter of co-constitution: no issue, no public [and vice versa]. This leads Dewey to understand democracy as the process of the simultaneous construction of publics and issues, whereby people regain a measure of control over issues their delegates do not take proper care of. Publics and issues are performed, constructed, fabricated – not given. Their articulation and their assemblage require hard work. There is not one – given – Public, but a multiplicity of publics that changes shape in relation to the issues they frame. And also, in relation to each other.
Dewey’s publics differ from Arendt’s public sphere. His publics are more empirical and contingent and they have less continuity. In fact a successful public will resolve its issue and cease to exist as such. However, both require individuals who take the risk of raising their voice, contesting common sense and – more importantly – initiating the construction of a new common sense around what they present as an issue. Dewey seems less concerned with opposing ‘the social’ with ‘the public’. His definition of democracy demonstrates a fundamental trust in the wisdom of crowds [to be distinguished from a naïve wisdom of ‘the Crowd’]. Like Mouffe (2000) in political theory and Rip (2003) in constructive Technology Assessment, Dewey trusts the outcome of agonistic decision-making processes. His publics are always under construction – they thrive on, contest and challenge whatever pretends to represent ‘the social’. They ground a natality in the midst of ‘the social’, a possibility for radical reinvention of what is taken for granted.

What interests me here is how we – a public constituted around the issue of ONLIFE – can contribute to the design, the engineering, the construction of an ONLIFE that affords the formation and un-formation of publics, while protecting and cherishing the opacities of the individuals that make these publics. In fact I believe that the draft Regulation of Data Protection holds several gems that may actually provide stepping stones to such an ONLIFE. In the third part of this contribution I venture into the radical choices it presents and the bridges it builds between legislation, architecture, social norms and market forces (Lessig 2006).

C. Legal Protection by Design: a novel social contract?

C.1. The nature of the social contract

Having explained, in the first section, the challenges of an environment that comes due to a ubiquitous and pervasive layer of machine learning, I have put forward, in the second section, the question of what this means for the public, the social and the private. My conclusion was that we need to construct an infrastructure that allows for a plurality of publics, a choice of exposure and places to hide. Such an infrastructure cannot be taken for granted, it will not appear of itself, nor will it grow organically or ‘naturally’ from the computational layers we are currently putting in place.

The social contract that combined the idea of limited government with – ultimately – representative, deliberative and participative self-government was the result of a historic bargain (Nonet 1978). This bargain sealed the autonomy of the law in relation to politics on the condition of non-interference; the independence of the courts thus combined with the monopoly of the legislator to enact the law. We can summarize this as the legislator writing and enacting the law, and the court speaking and interpreting the law. Let’s invoke Montesquieu’s often misunderstood maxim: \textit{iudex - non rex - lex loqui}. Not the king but the judge speaks the law (Schönfeld 2008). This was an attack on the medieval maxim that attributed all powers to the king: \textit{rex lex loqui} (the King speaks the law). The division of tasks that follows from the
The historic bargain between enacting and deciding the law was based on the socio-technical infrastructure of the printing press; the checks and balances of the Rule of Law depend on the sequential processing of written codes that can be debated, interpreted and contested by those under their rule. The fact that the courts have the final word in case of a conflict guarantees a measure of due process, making effective the fundamental rights that are part of the social contract. This is not to say that the printing press ‘caused’ the Rule of Law, but to suggest that it created a socio-technical infrastructure conducive to a specific division of tasks between the differentiated powers of the state. This division has specific temporal dimensions: the court speaks after the legislator enacts; courts are bound by the law enacted by the legislator, while in turn the legislator is bound by the interpretation of the courts – the circle is virtuous, it constitutes countervailing powers and creates room for both enforcement and contestation. All this is part of modernity. It depends on the internal division of sovereignty. Ultimately it depends on the monopoly of violence which is at the core of the operations of sovereignty; effective protection of fundamental rights is only possible if the state can enforce them. Even if they must be enforced against the state itself.

C.2. Protecting modernity’s assets: Reconstructing the social contract

In his Die Aufklärung in the Age of Philosophical Engineering Stiegler (2012) accepts the challenge introduced by Tim Berners-Lee, who argued that ‘we are not analysing a world, we are building it. We are not experimental philosophers, we are philosophical engineers (Halpin 2008).’ Berners-Lee is not merely describing the activities of the architects of the world wide web he invented. He is calling them to account for the impact of their engineering on the constitution of mind and society. He is inviting them to build a new res publica. Stiegler is more careful. He suggests that digital technology is a pharmakon: ‘it can lead either to the destruction of the mind, or to its rebirth (ib. 2).’ Referring to Wolf (2008) he notes that the transition from the reading mind to the digitally extended mind entails substantive changes to the composition and behaviour of our brains. Though these changes may be cause for celebration, they also threaten the constitution of the self. In the course of his manifesto Stiegler reiterates the crucial question of what we need to preserve as a valuable heritage of the era of the ‘reading brain’ (Wolf 2008). I want to hook this up with the need to reconstruct the social contract, recognizing that the social contract is a modern invention enabled by the ICT infrastructure of the printing press.

Though we might wish to declare ‘Game over for modernity’, this may require us to give up on the social contract that protects against immoderate government. Let us remind ourselves that the end of modernity will not necessarily bring the end of totalitarian governance. The hidden complexity of computational layers in fact affords refined and invisible manipulations that may be closer to the totalitarian nightmares of Kafka’s Trial (Solove 2004) and Foster’s Machine (Forster 2009) then to the dictatorial schemes of Big Brother watching you. Stiegler (2012) notes that ‘the spread of tracea-
bility seems to be used primarily to increase the heteronomy of individuals through behaviour-profiling rather than their autonomy.' The ‘old-school’ social contract will not necessarily survive when cut lose from the ICT infrastructure of the printing press. The idea of the social as a distinctive sphere is in fact typical for modernity’s reliance on information and communication technologies that sustain a further distantiation and differentiation of societal spheres. Oral societies do not have written constitutions capable of keeping their economic and military leaders in check, they require continuous calibration that entails a persistent threat of violence to keep the vicious circle of private revenge at bay (Hoebel 1971). Societies of the manuscript (the handwritten script) have no means to contest written laws for the majority that does not read or write; these societies thrive on the monopoly of the class of scribes that buffers between ruler and subjects, thus also protecting its own monopoly (Glenn 2007). Only the printing press provides the specific affordances conducive to the agonistic framework of representative, deliberative and participative democracies under the Rule of Law (Hildebrandt and Gutwirth 2007). My aim would therefor be to mine the gems produced by modernity’s dependence on sequential thinking (Wolf’s era of the reading brain) and its temporal structure that favours reflection over reflexes (again, Wolf’s era of the reading brain). This entails an attempt to engage with the benefits of modernity while passing over the lost territory of necessarily hierarchical and linear models of social life. To the extent that hierarchy or linearity protect us from chaos and contingent power games, we will have to reconstruct and reengineer them and to keep them in bounds in function of the purpose such hierarchy should serve.

A hierarchy that organizes countervailing powers may save us from the totalitarian rule of transnational computational decision-systems. At the same time we should acknowledge that the dreams of early cyberspace utopists have not come through; the nation state has not lost its bearing and territorial jurisdiction has not become meaningless (Goldsmith and Wu 2008). This requires vigilance in the face of potential attempts to turn cyberspace into a set of Walled Gardens that might reinforce not merely totalitarianism but also tyranny (Mueller 2010). We must investigate how the novel affordances of cyberspace can be set free as well as constraint, in such a way that they foster a fair distribution of capabilities (Cohen 2012). This urges us to take into account that cyberspace may change the game for modernity’s incentive structure, whereas it still nourishes on the system of legal-political checks and balances that was generated by modernity’s socio-technical infrastructure.

C.4. Technology Neutrality and Legal Protection by Design

One way of dealing with the implications of cyberspace as a game changer is to integrate legal protection into its socio-technical backbone: its hardware, software and the numerous protocols and standards that enable and constrain its affordances. I have coined this ‘legal protection by design’, connecting the concept to research communities working on value-sensitive design (Flanagan, Howe, and Nissenbaum 2007), constructive technology
assessment (Rip, Misa, and Schot 1995), upstream engagement with scientific research (Wynne 1995), the concept of nudging in behavioural economics (Thaler and Sunstein 2008), privacy impact assessment (Wright and de Hert 2012) and privacy by design and default (Cavoukian 2009; Langheinrich 2001). Contrary to notions like techno-regulation this is not about how to technically enforce legal compliance, because legal problems cannot be solved by technical solutions.

The concept of legal protection by design refers to novel articulations of fundamental legal rights into ICT infrastructures other than the printing press. Both lawyers and policy makers tend to display the Pavlov reflex of writing and enacting new laws when legal problems occur, whereas cyberspace easily turns written law into a paper dragon. Modern law is articulated in the technology of the printing press and in cyberspace its monopoly seems hard to enforce. At the same time, however, the administration has developed techniques to automatically enforce written administrative rules by translating them into automated decision systems. Social security, taxation and numerous permits are now granted or imposed on the basis of such decisions. Legal protection by design must therefore not be confused with techno-regulation or technological enforcement of legal compliance (Hilbrandt 2011b). Law is not administration, politics or policy. Legal protection by design instead implies that written legal rules and their underlying unwritten legal principles develop a new type of technology-neutrality. Other than some authors suggest, technology neutrality requires a keen eye on the normative implications of technological developments (Reed 2007; Hilbrandt 2008 and 2011b). Wherever a technology changes the substance or the effectiveness of a right, its articulation must be reconsidered to take into account how we wish to reconceptualise and/or reframe the right within the network of related rights and principles. The socio-technical infrastructure of cyberspace often affects the network and the context of sets of rights; e.g. rights to compensation based on tort or contract as well as rights to privacy, due process and non-discrimination. Technology neutrality therefor requires a lively debate amongst lawyers but also generate a similar debate amongst the architects of cyberspace on how to reinvent, to reengineer and to redesign democracy and the Rule of Law in the ONLIFE environment.

C.5. The proposed Data Protection Regulation

Let's now be practical. Though some inhabitants of the ONLIFE world may claim that data protection is boring and concerns an outdated attempt to revive ‘old-school’ privacy, I would argue that the legal framework of Data Protection is particularly well tuned to the data-driven environment of cyberspace. Whereas the value of privacy may indeed have been an affordance of the era of the printing press (Stalder 2002), we should not sit back to sing its requiem but need to assess how it can be re-invented as a dimension of the ONLIFE habitat. The Fair Information Principles that inform the legal framework of data protection seem particularly apt to cope with the flux of de- and re-contextualization that drives cyberspatial innovation (Kallinikos 2006). So far, however, these principles were articulated as paper
dragons, trailing an irritating bureaucracy while at the same time enforcement seemed an illusion due to the lack of teeth, money and personnel of the data protection supervisors. Compliance was a matter of costs, to be taken into account after new business models were set in place.

The proposed Regulation is a game changer. It establishes a new incentive structure and is based on a salient understanding of law’s need for effective [not theoretical] technology neutrality. The Regulation presents the combined force of a mandatory data protection impact assessment, data protection by default (data minimisation at the level of applications), data portability (enabling an effective right to withdraw consent without losing the value of self-generated profiles), the right to forget (requiring effective mechanisms to achieve a reasonable measure of erasure of one’s personal data if no legal ground applies for their processing), rights against measures based on profiling (a right to object to being subjected to automated decisions and transparency rights as to the existence of such measures and their envisaged effects) and finally data protection by design (which imposes the duty of adequate mechanisms for compliance on commercial and governmental data controllers). All this would have no effect if the proposal had not ensured efficient mechanisms to incentivize the industry to actually develop data protection by design: the liability regime is inspired by competition law (fines of maximum 2% of global turnover) while the burden of proof per default rests with the data controllers. This may finally create the level playing field that challenges companies and governments to develop intuitive and auditable transparency tools. ONLIFE inhabitants will then have the chance to play around with the system, exploring and inventing their identities in the interstices of the hybrid social contexts that shape their capabilities. This should empower them – us – to establish a new hybrid social contract that enables a plurality of publics, a choice of exposure and places to hide. Writing did not erase speech, but it changed the nature of speech (Ong 1982); computational layers will not erase writing, but it will change the nature of the reading mind. This may be a good thing, but that will depend on how we invent the infrastructure that will invent us.
Bibliography


- Dwyer, Catherine. 2009. “The Inference Problem and Pervasive Computing”. In *Proceedings of Internet Research 10.0*. Milwaukee, WI.


• Hildebrandt, M. 2011a. "Who needs stories if you can get the data? ISPs in the era of big number crunching". Philosophy and Technology.


• Stalder, Felix. 2002. "The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy." Sociological Research Online 7 (2).


