

Vrije Universiteit Brussel

From the Selected Works of Mireille Hildebrandt

2006

Privacy and Identity

Mireille Hildebrandt



Available at: https://works.bepress.com/mireille_hildebrandt/6/

Please, do only refer to the published version:

**Hildebrandt, M, 'Privacy and Identity in
E. CLAES, A. DUFF & S. GUTWIRTH (eds.), *Privacy and the
criminal law*, Antwerp/Oxford, Intersentia, 2006, 61-104 . (ISBN 90
5095 545 2)**

Privacy and Identity

Mireille Hildebrandt

1. The gift of privacy

Some time ago I visited New York. After returning to the Netherlands I read the essay by E.B. White about New York as he experienced it just after the second world war. On the first pages he celebrates the 'gift of privacy' one can experience walking around Manhattan.¹ This hit me as a profound truth: as in other metropolitan cities, one can acquire an acute sense of privacy in the middle of New York that can go beyond the privacy of one's own home—beyond solitude or exclusive intimacy. It is somehow related to anonymity, to the public eye and to a sense of security. I doubt that I would feel very private if I felt threatened or if I was recognized at every corner (as I am in the village where my parents moved after raising me in a city, and as I would be if I were a celebrity – the 'birth' of the right to privacy in the US was very much connected with the exposure of celebrities in the press).² The curious thing is that the public gaze, however uninterested, however much the opposite of intimacy, is part and parcel of this acute sense of privacy. Does this sense of privacy refute the idea that CCTV cannot be an intrusion on privacy as long as it only records what happens in public space? Could it be that privacy is not equivalent to private life as opposed to public life? What then, is the difference between CCTV and the gaze of the people you mix with on a busy street? Could it be the fact that while those who have access to the screen can see you, you cannot see them? Or should we locate the difference in the fact that the CCTV images can be stored and replayed, maybe even sold and linked with other images? Perhaps the fact that we cannot see those that can see us disturbs our immediate sense of privacy, while the storage, processing and selling of this type of information may go unnoticed, thus lacking any impact on our

¹ White E B (1999), *Here is New York* (1949, reprint 1976), with an introduction of Roger Angell. New York: Little Bookroom.

² Smith R E (2004), *Ben Franklin's Website: Privacy and Curiosity from Plymouth Rock to the Internet*. Sheridan Books: 121-153.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

sense of privacy for the moment. However, the knowledge that is constructed out of these data could very well have a lasting influence on the choices I make, even without any awareness on my part. Does it make sense to understand such knowledge construction as an infringement of my privacy?

In this paper I would like to explore the gift of privacy in counterpoint to David Archard's interesting analysis. I will start with some reflection on attempts to define strict boundaries for the concept of privacy (s. 2). As privacy concerns the relationships between a self and her environment (other selves), I will emphasize the relational aspect of privacy and the importance of a concept of social/phenomenological/embodied space for an adequate understanding of privacy (s. 3). Building on this, I claim that privacy is not merely about the exchange of or access to personal information, but about identity-building and identification. To explore this further, I will use Paul Ricoeur's study of identity, placing personal identity at the nexus of the two meanings of identity: *idem* or sameness and *ipse* or selfhood. Following Varela and Deleuze, I will then problematise the idea that identity has a fixed nature and argue that privacy can best be understood as the virtual and actual space needed to continuously reconstruct the self in the face of ever changing contexts (s. 4). The relationship between privacy and the divide between public and private is more complex than Archard seems to recognise. This applies not only to public and private space but also to the relationship between privacy and constitutional democracy. Privacy, at the nexus of negative and positive freedom, is a precondition for people to participate as citizens in democratic processes (s. 5).

2. Defining privacy: concept, phenomenon, right or value

Following Shoeman,³ Archard stipulates that (1) a definition should be able to cohere different claims to the right of privacy in the sense that they share a common significant and substantive feature and (2) a definition should avoid specifying a right to privacy that is derived from one or a set of moral principles that are also the grounds for some other right. In thus endorsing a cartesian method, developing an idea of privacy that is 'claire et distincte', Archard and Shoemann rob themselves of salient insights into the rich and fuzzy nature of phenomena like privacy. In everyday conversation privacy is strongly related to intimacy (referring to a relational space that is close and exclusive), and also to autonomy (referring to the control we like to have when negotiating boundaries with our environment) and human dignity (referring to the equal respect due to every human person). Archard's method of definition demands that we look for privacy somewhere else, disregarding the fact that maybe intimacy, autonomy and human dignity can be aspects of privacy. The same applies to the demand that the right to privacy should not be reducible to some other interest such as liberty, individual property, intrusive nuisance, bodily integrity etc..

Instead of investing energy in a strict definition of privacy, I would rather take notice of the open texture of words like privacy, being aware of the inherently

³ Schoeman, F (1984), 'Privacy: Philosophical dimensions of the literature', in idem (ed.), *The Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

underdetermined nature of terms that refer to interactional, relational and dynamic phenomena such as privacy. If privacy is understood in a dynamic sense, as the habits that people develop to negotiate boundaries with their environment, it would be more interesting to develop the concept of privacy in terms of a *type* that coheres an indeterminate set of *tokens* that are related by at least a family resemblance in Wittgenstein's sense. This means that these different tokens do not necessarily share a common feature but are nonetheless related, like ancestors or cousins of the third degree are related to me even if we don't share any genes. In that case concepts like human dignity, autonomy, intimacy, liberty, home, family, correspondence, intrusive nuisance, bodily integrity and public slander or defamation of character may turn out to be conceptually linked to the concept of privacy, without the implication that privacy can be reduced to any one of them and even without claiming that every manifestation of privacy is linked to every one of those concepts. It does imply, however, that it would be silly to demand that the concept of privacy be defined outside the scope of these terms. The concept of privacy simply refers to both more and less than each of these concepts; the challenge is to taste and probe the complex network of relations between these terms to find out how and in which cases and contexts they are related to what we call privacy.⁴

One of the problems we face here is a possible confusion between the *concept* of privacy, the habits/practices this concept refers to (the *phenomena*) and the *right* to privacy. Could it be the case that the concept of privacy is vague, while to claim a right to privacy such vagueness would have to be eradicated? This is an interesting proposition, because legal certainty seems to demand clear and distinct articulations of that to which one is entitled. Archard's point could be understood as the rejection of a right to privacy, precisely because privacy is too indeterminate a concept to produce the determinate legitimate expectations that fit an individual right. Privacy can then be seen as a *value*, something to be protected, and for this protection we can use a whole range of legal instruments (legal obligations, individual rights and liberties), that define in a much more precise manner what exactly one is entitled to. Whether using the term 'value' for privacy reduces or increases the confusion between concept, phenomena and right is debatable. But I agree that we can speak of privacy as something we value, a move that brings in the normative perspective and clearly indicates common ground between many writers: privacy is something of value, which is worthy of protection if violated. Perhaps at some point it is interesting to speak of an *entitlement* to privacy, that can be claimed by means of a variety of individual rights for citizens and safeguarded by means of a variety of obligations for the state – all part of the architecture of a vital constitutional democracy.

⁴ This concerns not only the concept of privacy but also the right to privacy. Cf. the way the ECHR explains the different conditions that constitute a fair trial in the sense of art. 6 ECHR. ECHR 21st February 1975 A-18, par. 28: 'It [the first paragraph of art. 6 ECHR, mh] enunciates rights which are distinct but stem from the same basic idea and which, taken together, make up a single right not specifically defined in the narrower sense of the term'.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

3. Privacy and information

3.1 *The information of embodied space*

When defining privacy Archard first indicates a commonly used definition: 'limited access to a specified personal domain (understood as personal information: the set of true facts that uniquely defines each and every individual)' (this volume, p. xx). In this definition the personal domain seems to refer to personal space as important for privacy, and in the explanation we see a reference to the unique definition of a person or, in other words, to identification. I will return to the issue of identification in the following section; here I will discuss the relevance of the personal domain for an adequate understanding of privacy. In the course of his paper Archard rejects the reference to personal space, because according to him zones of secrecy, anonymity and intimacy all stand for informational non-disclosure and can better be defined in terms of *limited access to restricted personal information*. This is actually the definition of privacy he defends as his own. As to the argument that there is a relationship between privacy and invasion of one's body space, he remarks that such invasion may be very unpleasant but as long as one is not actually touched this is a nuisance and not a violation of one's right to privacy. Here we see a confusion between the definition of the *concept* of privacy and the definition of the *right* to privacy. Not every violation of privacy is necessarily a violation of the right to privacy, since this right is obviously restricted, as all legal protection is. On top of that a right to privacy can – in specific circumstances – be overruled by the public interest, if necessary in a constitutional democracy. I don't think anybody defends an absolute right to privacy, even if the substance of the right should not be overruled by a state that claims its own interests as public interest, or a state that persistently 'forgets' that infringement of privacy in the end constitutes infringement of personal security.⁵

Unlike Archard, I think that the concept of space is important for privacy, though not in a naturalistic sense. Space is a crucial source of perceptual information that allows a person to move around and fit into her environment, to interact with it or even to reshape it. In fact very interesting research into privacy has been conducted by environmental psychologist Irwin Altman.⁶ He demonstrates, from a comparative perspective, how embodied space and privacy are intricately interwoven. For instance, the actual construction and composition of the home and the family (both the building and the people that live together, such as the nuclear or extended family), impose specific constraints on the way people construct their privacy. Altman defines privacy as a matter of *dialectical boundary control*.⁷ This boundary control does not

⁵ Art. 8 European Convention of Human Rights. The crucial issue here is that public interests should not be able to override a right to non disclosure in such a way that the right is no longer effective.

⁶ Altman, I. (1975). *The Environment and Social Behavior. Privacy Personal Space Territory Crowding*. Monterey, Brooks/Cole 1975, often referring to Alan Westin's *Privacy and Freedom*. For a phenomenological study of information technologies see Ihde, D. (2002). *Bodies in Technology*. Minneapolis London, University of Minnesota Press; and, De Mul, J. (2003). "Digitally mediated (dis)embodiment. Plessner's concept of excentric positionality explained for cyborgs." *Information, Communication & Society* 6(2): 247-266.

⁷ Altman defines privacy as 'selective control of access to the self or to one's group' (Altman :18) and elaborates on this in terms of social units, dialectic quality (privacy is both about opening and closing the self to others), optimization between desired and achieved privacy and finally as a boundary regulation process (Ibid:21-32).

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

necessarily involve intentional disclosure of propositional knowledge about a person, but rather an ongoing process of shifting one's boundaries in relation to information 'read' from the social and tangible environment. For instance, the fact that people are forced to live together in a limited space without much possibility of being on one's own can lead to a certain closure or reservation. In such situations it can happen that people do not show any emotion or even expression on their face. This does not indicate an empty emotional life but is a particular way of maintaining a desired level of privacy. Altman's comparative perspective on privacy sheds new light on the example Archard gives of sensory and cognitive access to him 'having heterosexual sex with Y' (p.xx). One should realise that many people in the world live in a home/family situation in which sensory access to their parents, brothers or other relatives having sex is unavoidable, since they sleep in one room. This 'sensory access' influences their behavior in terms of privacy. It does not mean that they have no privacy, but that they find other ways to protect their boundaries.

3.2 Identification technologies; sensory and cognitive access

A crucial element in Archard's paper is the distinction he makes between sensory and cognitive access to information. He rightly claims that in many cases cognitive access to certain information is not a violation of one's privacy, whereas another person having sensory access to the same information could indeed be an unpleasant or even degrading experience.

However, when we look at modern technologies, like webcams, the distinction between sensory and cognitive access blurs, precisely because of the fact that 'the social space within which people operate is no longer identical to the physical space that is readily perceived'.⁸ Whoever watches individuals via a webcam or a CCTV-camera, has both sensory access and cognitive access. But the sensory access is mediated by a technology, thereby reducing the access. For instance, those that watch the screen cannot smell or touch those that are filmed, and the visual access itself is framed and thus limited. At the same time the access is enhanced by the extension of the space to which access is possible. A consequence of this is that a public is created that cannot be seen by the participants, producing a new asymmetry between those that observe and those that are observed. This asymmetry is distinctive of most advanced observation and identification technologies.

The case of the webcam raises the question whether the use of a webcam renders the space that is filmed public, since others can now watch what is happening and – if the images are stored – the category of others is undefined. Does the use of a webcam rule out an invasion of privacy, since it creates a public space, or does this depend on the consent of those being viewed? My first point here is that the answers to these questions are context-dependent: who is watching; who took the initiative; are these images stored; for how long; are they also processed; by whom; for what purpose; who has official access; who has unofficial access; are the images sold (pornography);

⁸ Bellotti, V (2001), 'Design for Privacy in Multimedia Computing and Communications Environments', in: *Technology and Privacy: The New Landscape*. Cambridge Massachusetts: MIT Press: 73.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

or are they interpreted, classified and the information then sold (to whom, for what reason, on whose initiative)? My second point is that technological mediation of sensory access changes the nature of both the sensory and cognitive access and their relationship, by changing the space and the pace in which both perceptual and conceptual knowledge is accessed. Technologically mediated information thus actually constitutes simultaneously reduced and enhanced forms of both sensory and cognitive knowledge. This has obvious consequences for the way people are able to construct and protect their boundaries, as it may not be easy for those that are observed to access the *knowledge* that is produced on the basis of their 'data'.⁹ To understand the transformation of data into knowledge we must move beyond the mere collection of personal data by webcams, CCTV's, embedded sensors and other online and off line identification technologies. These technologies supply enormous amounts of data to so called *data controllers*. These data controllers exploit data bases in which the recorded data are aggregated; they run data mining software on these data to discover patterns or correlations (profiles). Such patterns contain new information about the habits, preferences and life style of the people whose data have been captured, called *data subjects*. In many cases this new information is not based on a hypothesis that is tested against the data in the database, but emerges after applying algorithms that produce correlations between often insignificant data. It may turn out, for instance, that lefthanded people are well represented in specific branches of employment, run into specific types of accidents, suffer certain types of diseases. This type of knowledge constitutes what is called a group profile: it consists of sets of correlations that indicate relationships between different data in terms of probabilities. If several group profiles are combined and correlated with personalised profiles, it is quite possible to produce knowledge about an individual person of which even this person is not aware (concerning consumer preferences, health-risks, career-developments or even the likelihood of becoming involved in criminal activities). Data controllers can sell or hand over the profiles to *data users*: the service providers or riskmanagers who use profiles to assess risks and opportunities. Thus access to personal data in a computerised intelligent environment is just the beginning of a process that generates 'knowledge' about groups and individuals who are most of the time both unaware of the collection, storage and processing of data, and ignorant of the opportunities this creates to construct of new types of knowledge. Those that 'offer' their data become transparent in a new way, while those that record and process these data are in fact invisible.

I think that the way Archard distinguishes between sensory and cognitive access is not adequate if we want to deal with the phenomenon of privacy in a technologically mediated world such as ours. Terms like 'sensory' and 'cognitive' can easily be taken to refer to the modernist gap between empiricist and rationalist knowledge, which has been criticised persistently as inadequate to describe the situated and embodied nature of both our perception and our cognition.¹⁰ As to sensory or perceptual knowledge, a

⁹ About the process of knowledge discovery in data bases (KDD) and the dangers for privacy and fair treatment, see Custers, B. (2004). *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Nijmegen, Wolf Legal Publishers.

¹⁰ As such both perception and cognition are inextricably tied up with each other in the body, see Varela, F. J. (1992). *Ethical Know-how*. Stanford, Stanford University Press: 1-21. An interesting account of this criticism in the light of biotechnology and ICT: De Mul 2003.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

more phenomenological interpretation can shed light on the changes in lived time and space prompted by the new technologies, in order to understand the impact of these technologies on the way people can construct their privacy. As to cognitive or conceptual knowledge, I think we should not underestimate the extent to which knowledge construction on the basis of as yet insignificant personal information (data) can have an impact on identity-building and is therefore relevant to the ability to construct and sustain our privacy.

4. Virtual identity: a central aspect of privacy

4.1 Privacy, identification and identity-building

In his definition of the concept of privacy Archard stresses two points. Privacy concerns (1) limited access – a persistent feature of all understanding of privacy – to (2) (restricted) personal information. He goes on to define personal information as 'true facts that identify the person as a unique individual' (p. xx). I would like to pause for a while to examine the relationship between privacy and identification, because I think that the core of privacy is to be found in the idea of identity – not only because in our information society it is precisely the advance of high-tech identification technologies that raises questions of privacy-protection, but also because the process of identity-building is what is at stake in privacy.

In their introduction to *Technology and Privacy: The New Landscape* Agre and Rotenberg suggest the following working definition of the right to privacy, referring amongst others to Roger Clarke's *digital persona*: **'the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity'**.¹¹ One of the interesting things about this definition is the apparent link between negative freedom (liberty), *freedom from*, and positive freedom (identity-building), *freedom to*. I will argue below that this link is a crucial aspect of privacy. Another salient element of the definition is the use of the term 'unreasonable'. This precludes an absolute rejection of privacy-invasions: not every possible constraint on identity-building is warded off by a right to privacy. Those that imagine that the law can provide absolute certainty will dislike vague terms such as reasonableness, but as a lawyer and as a philosopher I would claim such certainty is non-existent. The history of modern law indicates what happens if such a mechanical kind of legal certainty is sought. Begriffsjurisprudenz in Germany, legalism in France, stare decisis in England and legal formalism in the US all threatened to close the law against life as people experienced it in the second half of the 19th century. A strictly defined right to privacy will not be an adequate tool to protect the value of privacy, that – as we saw in s. 2 – is too complex and rich to be defined in strict terms.

¹¹ Agre, P. E. and M. Rotenberg (2001). *Technology and Privacy: The New Landscape*. Cambridge, Massachusetts, MIT: 7. Clarke, R. (1994). "The Digital Persona and its Application to Data Surveillance." *The Information Society* 10(2). Clarke basically wrote about what we would now call identity management by a data subject via an electronic agent (the digital persona) that regulates or even negotiates access.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

4.2 Narrative identity: sameness and selfhood

The most interesting part of Agre and Rotenberg's definition seems to be the recognition of identity as something that is both under construction and of central importance for matters of privacy. If you define personal information as a set of true facts that identify a person as an individual, you imply a static conception of identity: it presumes that the core of an individual can be fixed for identification (date of birth, nationality, eye colour, gender etc.). People are defined in terms of categories that apply to everybody. Such fixing may be necessary for an adequate system of identification, necessary to distribute access to a number of services in a welfare state and in an economic market. This is one side of the coin, concerning the establishment of a set of attributes that can individuate a person within a population. Such individuation is based on *sameness* (of the categories by which you specify the attributes of each person). It concerns identification from the perspective of a third person, it presumes objectification.¹² It is interesting to observe how both the state and the market put substantial effort into legal and technological means to locate and identify individual subjects. The beginnings of the state are rooted in the capacity to collect taxes (a government lives on the surplus others produce); the success of an economy that moves beyond subsistence level depends on markets and credit-systems (translocal trade demanding both trust and some instruments to hold debtors accountable). Both the welfare state and totalitarian states are even more concerned about tracing and monitoring their subjects, the first to allocate the right resources to the right people, the second to sustain total control. In a large scale and complex society characterised by mobility of persons, goods, services and capital, elementary forms of identification in the sense of individuation are preconditions for the functioning of both state and market. This in itself does not have to infringe our privacy.

The other side of the coin concerns something different: the construction of self-identity from the perspective of the first person. This type of identity presumes that humans are not *born* as individual persons, but *develop into* persons as they relate to their environment and interact with others. Developing into a person means that one is constituted as a subject, a *self*.¹³ The self lives at the nexus of two aspects of identity, that are never given: identity of the *self* (*ipse*) has to be claimed *versus others*, and the self has to be claimed as being the *same* (*idem*) *over the course of time*. The continuity of this relational self implies that the autobiography of the self is continuously re-written in confrontation with the flow of new events that shape one's perception of self, world and others.¹⁴ From this perspective, privacy can now be understood as the process of boundary negotiations that allows a person *to hold*

¹² On the difference between identification as specification (objectified perspective) and identification in a phenomenological sense (life world perspective), see Glastra van Loon, J. F. (1987/1956). *Norm en Handeling. Bijdrage tot een kentheoretische fundering van de sociale wetenschappen*. Groningen, Wolters-Noordhoff (*Norms and Actions. Contribution to an epistemological foundation of the social sciences*).

¹³ About the biological aspect of this constitution Varela writes in clear terms: the self never being 'at home', finished or given. See Cohen Varela, A. E. (2002). "Conclusion: "Opening"." *Phenomenology and Cognitive Sciences* 1(2): 225-230. Another interesting perspective from both biology and philosophy is Plessner's excentric positionality, see De Mul 2003.

¹⁴ About narrative identity at the nexus of *idem* and *ipse*: Ricoeur, P. (1992). *Oneself as Another*. Chicago, The University of Chicago Press.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

together while changing; it presumes some measure of autonomy, some real contact like intimacy and some space to rebuild the self in accordance with one's past while anticipating one's future. All this is for the most part not a conscious effort, it rather happens 'under the skin'; identity-building is not a voluntaristic project. But, unlike identification in the sense of unique categorisation, construction of the identity of the self implies indeterminacy, and privacy therefore implies the recognition of this indeterminacy.

4.3 *Virtual and actual identity; correlatable humans and correlated data subjects*

To understand how the collection, storage and processing of personal data (Knowledge Discovery in Databases) can impact on privacy, I will elaborate on the relation between privacy, freedom and the indeterminacy of self-identity.

There is an important difference between the way data users and computer scientists tend to regard the nature of the data they need for their computations, and the way biologists and philosophers like Francisco Varela describe the persons, events, actions or biometric 'substance' those data refer to. When Archard defines personal information as 'the set of true facts that uniquely defines each and every individual' (p. xx), he seems to imply that individuals can indeed be defined by means of a set of 'true facts' *that are given*. In that case the problem with personal information is restricted either to the fact that the data does not represent correctly these 'true facts', or to the fact that I can legitimately object to certain information becoming public or being transferred into the hands of others whom I do not want to have access. It is interesting to note – again – that privacy is not equivalent to the private in opposition to the public; my sense of privacy may be at stake when information concerning my person ends up in the hands of a private organisation that has no intention whatsoever of making it public. My objection may be simply that I consider this information as 'nobody's business', invoking my wish to be left alone. However, if I am aware of the knowledge that can be constructed with such data, I may rather fear the manipulation this knowledge makes possible. This is not only a matter of abuse, as the line between targeted servicing and manipulation is very thin. I may simply not want to be party to data flows that confront commercial enterprise or security agencies with this thin line. The bottom line of this account of personal information is, however, that it is a given, which defines your identity as a person. Following Varela, this presumption can be questioned.

Varela, a biologist and philosopher who coined the term 'autopoiesis' for the processes by which autonomous organisms organise and constitute themselves, moved into brain sciences later.¹⁵ He wrote about identity as a continuous process rather than a fixed state. He spoke of the body as 'the continual reconstitution of its emergent identities' and went on to say that 'identity resides nowhere, except in its autonomous constitution (...)'.¹⁶ In the language of speech act theory, claiming

¹⁵ Maturana, H. R. and F. J. Varela (1991). *Autopoiesis and Cognition: The Realization of the Living*. Dordrecht, Reidel, Varela, F. J., E. Thompson, et al. (1991). *The embodied mind : cognitive science and human experience*. London, MIT Press.

¹⁶ Cohen Varela 2001: 226.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

identity is a performative action, precisely because it is not a given, not out there and also not 'in here'. Perhaps Varela's most radical claim is the absence of a given identity 'in here', a stable unitary self that can be discovered by introspection. Though on different grounds and from different perspectives, Nietzsche and Freud had already come to that same conclusion. The point made by Varela and others, however, is *not* that the absence of a given identity implies that identity does not matter, that it is a fiction we can do without.¹⁷ Thinking *with* Ricoeur we could even say that this fiction is constitutive of our self.¹⁸ What this decentred concept of self-identity discloses is the fragile, underdetermined and open character of identity.

This – fruitful – indeterminacy finds beautiful expression in the work of Deleuze,¹⁹ where he discusses the difference between the virtual and the actual. For Deleuze the virtual is the multiplicity of possibilities inherent in the present, but not yet actualised. A seed, for instance, is the virtual of the tree that grows out of it, while the tree is the actual of the seed from which it grew. Actualisation – becoming a tree – depends on the interplay between the multiple possibilities of the seed and its environment, and ends up stabilising into one particular tree. Actualisation is always underdetermined. While partly determined by its virtual 'roots', there is an element of invention everytime the fit with the environment doesn't work. In that sense the tree and its environment are both in a simultaneous process of actualisation. The outcome of the process of actualisation is thus not predefined, as it would be if it were a mechanical process. *Virtualisation* – thinking the tree back to the seed – invokes the numerous possibilities that were not actualised.²⁰ Our problem is that when we think the tree back to the seed, we tend to think that the development of this particular tree was, after all, defined by a mechanical chain of causes that could not have brought about another tree. As Nietzsche wrote: after the fact we believe in other causes than we did before.²¹

When we look at the knowledge construction that takes place after our personal data have been collected, stored and aggregated we will find our selves represented as correlated data subjects. Such correlated data subjects or profiles 'could possibly be used against individuals without their knowledge, thus shaping their access to facilities, goods and services, also potentially restricting their movement and invading personal space. In fact, this would regulate their access to, and participation in, the European Information Society'.²² As is the case with all technology, profiling technologies are neither good nor bad in themselves, but they are never neutral. The impact they may soon have on our access to insurance, employment, education, credit and all kinds of information affects our personal space, the negative and positive freedom to reconstruct our identity and thus – in the end - our privacy. Not in the

¹⁷ Ricoeur 1992: 134-139, 167-168.

¹⁸ De Mul, J. "Het verhalende zelf. Over persoonlijke en narratieve identiteit." www2.eur.nl/fw/hyper/colleges/UnderConstruction/Literatuur/VerhalendeZelf.htm [Narrative self. About personal and narrative identity.]

¹⁹ Deleuze, G. (1968). *Différence et Répétition*, Paris: PUF. Lévy, P. (1997). *Sur les chemins du virtuel*. <http://hypermedia.univ-paris8.fr/pierre/virtuel/virt0.htm>.

²⁰ Ibid.

²¹ Nietzsche, F. (1822). *Die frohliche Wissenschaft*, par. 217.

²² Levi, M. and D. S. Wall (2004). "Technologies, Security, and Privacy in the Post-9/11 European Information Society." *Journal of Law and Society* 31(2): 1994-220: 211.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

obvious way that we are hindered by a public gaze or disclosure of trivial data; the collection of these data proceeds for the most part by means of a seamless ubiquitous process that is invisible. But in the meantime our options in life are mediated by profiles that seem to define us as correlated data subjects, even though these profiles can never be anything but virtual since they are based on our past behaviour or biometric 'substance'. Any conclusion drawn from that perspective is an anticipation. If we connect the virtual character of human beings as correlatable data subjects to Varela's concept of identity, we could say that the most interesting thing about human nature is its indeterminacy and the vast possibilities this implies: our non-essentialist essence is that we are correlatable humans before being correlated data subjects. Whatever our profile predicts about our future, a radical unpredictability remains that constitutes the core of our identity.

While this indeterminacy or unpredictability does not rule out predictions in terms of probability, it does constitute the paradox of our sense of self: on the one hand we have a sense of continuity, on the other hand we are aware of the possibility of change. This is the core of our sense of freedom. The next paradox is that while this indeterminacy cannot be overruled, it still needs protection. To actualise our virtual identity in constant interplay with other things and other people we need a certain kind of personal space that is tuned to the multiplicity of the virtual. We need a design of public and private life that does not constrain us on the basis of past habits and inclinations. This would replace Foucault's 'classic' normalisation by means of imposed categories by a new process of normalisation that starts from our own inferred preferences, disrespecting the need to be confronted with what we do not prefer or expect, the need for unexpected change and thus the need to organise a free space at the nexus of the public and the private.

5. Privacy and the public/private divide

5.1 Public debate in the private sphere; private life in the public sphere

This brings me to my last point: the way Archard talks about privacy in relation to the public/private divide. With Gutwirth and De Hert I think that privacy is a prime concern for the construction of the democratic constitutional state. If we think about democracy and the rule of law from the perspective of a relational theory of law that follows Montesquieu's advice to construct checks and balances into the basic structure of the state, the links between privacy and democracy can best be summarised by referring to the nexus of negative and positive freedom, as exemplified in Agre en Rotenberg's definition.²³ Identity-building is a condition of possibility for a strong civil society and – as Gutwirth and De Hert indicate, referring to Habermas and Arendt – the *public* debate within the *private* sphere is a precondition for the workings of a sustainable democracy. Privacy and freedom of speech thus seem to presume each other, and rights to privacy are not only a matter of private well-being. They are

²³ About such a relational theory of law, see Foqué, R. and A. C. 't Hart (1990). *Instrumentaliteit en rechtsbescherming*. Arnhem Antwerpen, Gouda Quint Kluwer Rechtswetenschappen (Instrumentality and Protection of law). Such a theory builds on a relational concept of the person, precluding dominance of either a liberalist individual or a communitarian state. Thus I do not seek the foundations of this conception of law in the liberal tradition with its emphasis on a modern, disembodied subject.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

instruments to (re)construct the preconditions for our democratic constitutional state. This means also that - as against what Archard seems to suggest – privacy-rights should do more than just defend citizens against abuses of state power.

It is important here to distinguish between three senses of the term public: (1) public space as opposed to spaces of solitude or intimacy; (2) the public as the domain of the state, opposed to civil society; and (3) the public good as opposed to private interests. About the first point I have already remarked that the mere fact that I enter a public space does not rule out a right to privacy: advanced identification technologies (including profiling and ambient intelligence) change our perception of social/phenomenological space. This makes it all the more important to investigate the privacy one can build into public spaces²⁴ and the publicness of private behavior.²⁵ On top of that, as we have seen above, the knowledge that can be built on the basis of data gathered in public spaces may impact on our privacy when used to deny access to information, goods or services, even if this is done with nothing but good intentions.

5.2 *Privacy as a public good*

As to the second and third meanings of ‘public’, Archard talks about a simple trade-off between governmental access to non-restricted, mostly cognitive personal information on the one hand, and presumed effective anti-criminal measures on the other hand. He finds no problem here, apart from possible abuse of state power. On top of that he proclaims that a person 'fearful of her own decisions, or of acting on them, merely because others know what she would rather keep secret has a weak personality (...) her own nature, and not the loss of privacy, is what incapacitates her' (p. xx).

In a constitutional democracy, the government should be sensitive to unreasonable constraints on identity-building. This is a matter of the *public good* because democracy needs citizens who will form publics to make an issue of what affects their lives, every time representative politics fails to take their interest serious.²⁶ Such interplay between participative and representative politics only works if citizens find ways to assess the virtual or correlatable character of their identity, thus opening possibilities for change and new configurations of what holds them together as a democracy. Unreasonable constraints on identity-building are not confined to dealings between a government and its citizens. From the perspective of a relational theory of law, it is a task for the state to prevent both its government and other dominant centres of power from imposing unreasonable restrictions on identity-building. What is equally important, however, is that the point of intervention should not be the moment at which abuse is discovered, but long before that. As we have seen, the invasion of privacy that takes place with profiling and ambient-intelligence practices does not depend on abuse, but on the way these technologies impact on identity-building. After all, the knowledge produced by these techniques can be used to give people reasons to

²⁴ See the remarks on New York's gift of privacy above.

²⁵ Relevant in the case of both webcam & CCTV.

²⁶ Latour, B. (2005). From Realpolitik to Ding politik - or How to Make Things Public. *Making Things Public - Atmospheres of Democracy*. B. Latour and P. Weibel, MIT Press.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

rebuild their identity in ways that turn them into profitable consumers, assimilated foreign residents or – more generally – citizens who fit well into the scenarios of our policy-makers and marketing managers. Indeed, the effects of these advanced technologies should not be described in terms of weak or strong personalities, but in terms of their impact on identity-building, citizenship and democracy.

6 Conclusion: privacy, identity and the criminal law

Privacy concerns the freedom from unreasonable constraints that creates the freedom to reconstruct one's identity. As such it is intimately connected to the ideal type of the constitutional democracy, because this depends on citizens who claim their freedom to build a shared life world.

As far as criminal law is concerned this seems to imply an entitlement to privacy that – in the form of a human right to the protection of our private life - can overrule criminal investigation (depending on the circumstances), and an entitlement that demands the criminalisation of certain actions that illegitimately invade our privacy (unlawful entry; ill-treatment by those who hold power over others, whether state official, parent or employer; disclosure of sensitive personal information or of communication that was meant to be kept secret, etc.). I do not think Archard would disagree here, even if he may deny that such forms of criminalisation are grounded in a right to privacy.

More interestingly, the advance and proliferation of identification technologies create new challenges to our conceptualisation of privacy. What is at stake is not so much the disclosure of insignificant personal information to marketing organisations or justice authorities, but the impact of the knowledge constructed on the basis of these data as they are collected, stored, aggregated and correlated. Here the worry should be that the profiles generated by these types of technologies begin to determine decisions taken in the fields of criminal investigation, forensic evidence, judgement, sentencing and parole. The application of profiles constitutes a form of actuarial justice, thus promoting a way of thinking in terms of aggregated risks rather than listening to the particular story of an individual suspect or convict.²⁷ Opposing such actuarial justice as an infringement of privacy does not, of course, mean that I would rather believe whatever the suspect or convict tells. It does mean that to take the criminal law seriously in a constitutional democracy implies taking seriously the voices of those who have (allegedly) violated the law. The privacy of all citizens, their freedom from unreasonable constraints on the construction of their identity, applies equally to suspects and convicts. The new type of knowledge implied in these profiles demands that we think twice about the way we organise our public and private space as far as the collection of personal data is concerned.

²⁷ Hudson, B. (2003). *Justice in the Risk Society*. London Thousand Oaks New Delhi, Sage:40-78.

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006

published in:

Erik Claes, Anthony Duff, Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia 2006