No fear or hope but new weapons: a deconstruction of privacy

By Matthijs Kouw, Lizette Pater and Edo Schreuders

Abstract
In debates about privacy and technology, privacy has always been treated as a concept of which the content was more or less fixed. Instead of treating privacy as a given, we will take a step back in the discussion around privacy and problematize its apparent rigidity, thereby hoping to clarify the relation between privacy and technology. In order to do so, we will offer an unpacking of the conceptual implications of 'new' technologies, concentrating on the theme that it decontextualizes the subject's behaviour and identity.

1. Introduction
In this paper it will firstly be explained how the common-sense notion of privacy is a result of liberalist dichotomies. The liberal public and private dichotomy presupposes a fixation of privacy as an ontological category. Secondly, unveiling this ontological rigidity of privacy leads to a discussion of the impact of technology on our identities. Biometrics serves as an example to explain the way in which our identities are being constituted by discursive practices. In conclusion, it will be discussed, that when we describe our identities in terms of contextuality, the question arises whether or not privacy still has a function after the supposition of the stable core of subjects has been refuted.

2. Privacy in the liberal framework
In 1890, Warren and Brandeis famously formulated privacy as 'the right to be let alone'. This view, which can probably be seen as the first thorough systematization of the concept of privacy, has had an important position within the debate on privacy ever since [Gutwirth 1988: 15]. Despite its supposedly universal claim, this view clearly reflects a very limited conception of privacy, namely one that perfectly fits the liberal atomistic individualism that perceives of the individual as in permanent conflict with society (hence this negative definition of privacy).

This liberal doctrine is that upon which most Western democracies are based. It conceives of the human subject as a free and autonomous individual. A sphere of personal freedom is ascribed to this subject, which is thereby allowed to occupy a carefully circumscribed realm of individual responsibilities that is devoid of intervention from the public realm. The bedrock of this conception of the subject is provided by the humanist view that provides a fixed and carefully outlined core that can be inserted into a variety of contexts. Thus, a subject provides a stable means to multiple ends.

There should be as little interference with the individuals' decision-making as possible, so that even the state is barely entitled to have an influence. Yet, for the state to provide benefits to the citizens, it is needed that they acknowledge some interference imposed on their autonomy; they need to cooperate on a certain level, even if that means they have to agree on democratic principles that are not directly theirs. This problem of obligatory interference on autonomous decision-making for reasons of obtaining benefits for all citizens, can be solved by an exact mirroring of the dualism: a public sphere is installed to deal with the duties that citizens have towards each other, and a private sphere is installed where the citizen can practice its personal moral beliefs. This public and private dichotomy thus serves liberal principles: the recognition

that a state is needed to provide citizens with its benefits meets the autonomy of these citizens in the separation. However, as can now be seen, these spheres are only a construct to uphold the liberal state and do not follow any 'natural' conception of public or private spheres. Their instalment is not followed by a clear definition of how we should keep the spheres separated. '[L]iberalism is inherently ambiguous about the "public" and the "private"' [Pateman 1983: 281]. This dichotomous organization, as found in the Western liberal tradition, is based upon the 'ideal of impartiality': there is one universal principle that governs all particular phenomena, and that should be found by using rational, thus impartial, reasoning [see Young 1990]. This unification puts particulars in categories; it reduces all things to one principle. It wants stability, predictability, and certainty instead of a heterogeneous chaos of particulars. However, this craving for essence, for unity, fails. It inevitably creates a dichotomy instead of a unity, for there is always an unfitting 'Other', an outside as opposed to the inside. Everything that is valued by the Western tradition has its opposite, and it is this opposite of which we cannot get rid.

This serves the alleged neutrality of the liberal state, which claims to be impartial and rational, but that claim only works insofar all need and desire is kept in the private realm. The private sphere, which is valued lower than the public sphere, is reserved for social relations, the family and personal life. Sympathy and particular interests and needs of particular people can be be found here. The ideal of impartiality asks for a removal of particularities of context and affiliation from the public sphere.

Exclusion is the inevitable result of the hierarchical order that liberalism installs. Privacy as a furthering of the private-public distinction conforms to this exclusion. Seeking for privacy as a universal norm determines in a rigid manner how we should conceive of privacy without paying attention to the particular circumstances, to the context of each situation in which we would think privacy as applicable. Removing the context means that we let the universal principle decide. That principle, however, is not impartial, as it is meant to further an ideological, id est liberal, point of view.

This ideological conception of privacy can be traced back to the process of 'individuation', as described by Foucault in his *Discipline and Punish*, which lies at the very basis of liberal thought: the systematical gathering and organization of information about people, thereby creating (autonomous, atomistic) individuals. Special sites of architecture are designed in order to systematically obtain the information needed [see Foucault 1979]. The claim on privacy arose from this social order as the determining factor that set the borders between different realms of individuation. The (alleged) autonomous, sovereign individual needed the illusion of being in charge of setting the borders between the state and his private life: *privacy as gatekeeper*. However, this system penetrates and rules all actions of the subjects, so that the claim on a 'private' life is in fact an illusion, as that private life is as constituted by the social order as the public life. Yet, privacy is from a liberal point of view seen as a form of resistance against the individuating power, in terms of *hiding* from it ('the right to be let alone').

3. A contextual approach

Positioning privacy in the frame of liberal thought reveals it as a historically contingent and constructed matter. However, in the debates surrounding privacy there is, in a line that can be traced back all the way to Warren and Brandeis, the tendency to treat privacy as an ontologically stable concept or some sort of natural or even metaphysical right simply to be found in human nature. Thereby the question at hand is begged, namely: how is privacy being articulated in

particular social contexts? The treatment of privacy as ontologically given instead of relational, is problematic in two interrelated ways:

Firstly, a treatment of privacy as an ontologically fixed concept is unable to deal with recent technological developments. We cannot rely on the liberal meaning of privacy based as it is on the separation of the public and the private sphere, since new technologies blur this distinction. Take for instance the proliferation of surveillance cameras. These cameras bring private elements into the public sphere: we find our 'public' identity to be suddenly 'privatized'. Taking into account that surveillance cannot properly be explained in terms of this traditional public-private distinction, the question arises if this distinction, in a larger perspective, is still tenable. Instead of relating privacy to the traditional distinction of public and private, we might better consider doing away with these concepts altogether.

And secondly, treating privacy as a given leads to a very rigid conceptualization of technology. This results in a negative or at least problematic stance towards technology: technology is said to threaten the integrity of our human subjectivity, by intruding our privacy or by alienating us from our supposedly real selves. This technological determinism ignores the profound effects technology has on our human subjectivity: technology is not simply given and as such at our disposal. Technology should not be conceptualized as being merely a product, but needs to be understood in terms of the effects that it itself produces.

In opposition to these two problems we will argue that neither privacy nor technology is to be seen as isolated and ontologically fixed. We should perhaps better regard both privacy and technology as *contextual*, as '*in situ*'. The relation between technology and privacy is not a one-way street: neither are we completely determined by technology and is it an evil that threatens the presumed integrity of our human subjectivity, nor is our privacy a haven of safety founded in our human subjectivity from which we can judge technologies that are said to intrude our privacy. The question that then arises is, of course, which possibility exists for conceptualizing privacy in such a way that it is not founded on a notion of an autonomous self that is entitled to privacy and in such a way that we do justice to the profound effects technology has on our subjectivity? Seeing the relation between technology and privacy as a one-way street mystifies the context that is constituted in that relation. The focus should be on how privacy and technology form different symbioses that cannot simply be reduced to one component or the other. Instead of describing technological threats of privacy in terms of a presupposed notion of humanity, from which we are alienated, we should focus on the relation between privacy and technology.

4. Dataveillance in the control society

This relationality can be investigated from what Deleuze described as the control society. Whereas Foucault's panoptic disciplinary society, a concept often used in the debates on privacy, is more or less restricted to a architectural power over time and space (and can be associated to limited arrangements of time and space), Deleuze supplements this model with the idea of the control society [Deleuze 1997].

The control society needs to be described more in terms of information. The individual is no longer supposed to be a coherent physically localizable subject, but much more a 'dividual' that is nothing more than the sum of all the information that exists about it. The individual as data-source, a subject in informational terms. This makes surveillance a much more subtle practice. This can for example be illustrated by the attachment of so-called cookies to our electronic

identities, a form of electronic surveillance that goes on practically unnoticed when we use the Internet.

For the subjects in the society of control, what is important is not their number or signature (what Deleuze calls watchwords), but the *code* as a password. 'The numerical language of control is made of codes that mark access to information, or reject it. (…) Individuals have become "*dividuals*", and masses, samples, data, markets or "*banks*"' [Deleuze 1997: 311]. The physical substrate of the human being in the information society, or, society of control, has now lost its former importance: it cannot be reduced to this biological substrate, since this has lost part of its relevance in virtual (informational) communities.

Instead of focusing on bodies and their presence in a certain time and space constellation, the body functions as a producer of data and is only relevant in that aspect. It seems as if the grip that the system had on the integrity of the human body is only abandoned in so far as a deeper level of adherence, of penetration, could be attained. It has become of less importance what the body *does or* where the body *is*; the system is now on the lookout for *what facts or which data are produced*. Dividuation is the gathering of information without using a pre-set architecture or system (this in contrast with the aforementioned individuation with its special sites of architecture). Information is produced on a massive scale, and it is only afterwards that the streams of information are being channelled.

An increasing ubiquity of technological artefacts results in the production of vast amounts of data, which subsequently increases the need of deploying hierarchical stratificatory principles that order the data. It may be observed that the increasing emergence of techniques that serve to track user behaviour (such as the aforementioned cookies), also called dataveillance [Rodowick, 2001: 217], is one of the ways in which this ordering of data is realized.

5. Biometrics

Biometrics is an example of how this dataveillance and the claim on privacy are related. Biometric data is not a given, but articulated in a discursive practice. According to philosophers such as Foucault, Haraway and Butler, all of what we experience as part of our identities can in fact be seen as a text constituted through discursive practices. So much of an identity is discursive that we may call it a 'legible body', or a textually mediated physicality. The legible body represents a set of cultural codes that organize how it is to be understood, and that circumscribe a range of socially appropriate responses.

A discourse can be seen as a coherent form of using language within a certain period and environment. So there are medical discourses, scientific discourses, psychological discourses, etc. These discourses play a constitutive role in defining how we perceive of ourselves as human beings. Hence Foucault defines discourses as 'practices that systematically form the objects of which they speak' [Foucault 1972: 49]. Identity in that sense is the effect of discourses, of texts. This does not imply, of course, that identity itself is a text. Rather the way we perceive of our identity is 'textually mediated', that is: constituted through texts (i.e. medical files, scientific investigations, statistical information).

This 'legible body' is not prior to cultural inscription. As Haraway puts it: 'Bodies, then, are not born; they are made' [Haraway 1991: 208]. There is no body that is ontologically prior to the various functions through which it assumes social meaning. Bodies only become intelligible in conformity with recognizable standards of personalization-intelligibility. One cannot simply find meaningless bodies in nature: 'their boundaries materialize in social interaction; objects like bodies do not pre-exist as such' [Haraway 1991: 208, see also Butler 1999: 22]. That is why

Haraway mentions in her analysis of constitutions of the self in immune system discourse, that 'various contending biological bodies emerge at the intersection of biological research, writing, and publishing; medical and other business practices; cultural productions of all kinds, including available metaphors and narratives; and technology' [Haraway 1991: 208]. A body should be understood as 'a coded text, organized as an engineered communications system, ordered by a fluid and dispersed command-control-intelligence network' [Haraway 1991: 211].

An example of such an identity-constituting discourse can be found in relation to biometrics. The registration of specific physical characteristics of a person, as is done with iris scans, fingerprints, hand scans, voice recognition and facial recognition, can be said to form a 'biometrics discourse'. The way data is generated, stored, retrieved, processed and transmitted, has a constitutive effect on identity. It permits surveillance to 'move beyond paper files and digitized documents and to infiltrate the body itself' [Lyon 2001: 299]. The body, then, is transformed into a text, a password, a document for decoding. This may, according to Lyon, (re)constitute the body as a text: '[t]he emergence of body surveillance technologies (…) dispenses with cryptic words and numeric codes. Some part of the physical body -eye, hand, finger, face, voice- is presented to the verification machine. Another level of coding, beyond words and numbers, and relying neither on memory nor on the need to produce a card, *turns the body into a password*' [Lyon 2001: 297, italics ours, see also Lyon 2001: 299].

It is in this sense that the idea that biometrics is an ontologically neutral classification of facts that can be found 'in nature', or 'on a body', can be criticized. Because, as said above, when the intelligibility of a body is constituted by the biometric discourse itself, the quantification of biometric data can by definition not be a value free, neutral activity. David Lyon mentions in an essay an example with which this point can be illuminated. Kenneth Payne is an American citizen who qualified as a teacher in his forties. Because he suffers from atopic dermatitis, his skin is so blistered and peeled that his fingerprints are spoiled. In California all teachers need to pass a fingerprint test: no print means no job. So Mr. Payne cannot obtain employment. [Example mentioned in Lyon 2001: 308].

The point here is not that Mr. Payne is an exception that is not representative for the rest of the population. Rather the point is that fingerprinting can exclude otherwise intelligible persons. Mr. Payne does not have a biometric identity, but is the impossibility of such an identity. The existing biometrics discourse finds its limit in Mr. Payne, because he cannot be categorized within that discourse. The biometrics discourse that produces an intelligible biometric identity requires that certain identities cannot exist. Identities that fail to conform to those norms of biometric intelligibility appear as impossibilities. However, their proliferation provides critical opportunities to expose the limits and regulatory aims of that domain of intelligibility (Butler calls this a 'disordering practice' to the 'matrix of intelligibility', and points out how this provides critical opportunities to open up rival and subversive matrices [Butler 1999: 24]). When a biometric identity is assured through norms of a biometric discourse, that very notion of identity is called into question by the existence of those 'unintelligible' beings that fail to conform to the norm of cultural intelligibility by which persons are defined in the biometrics discourse.

Relating all this back to privacy, the following issues arise.
First of all, we need to ask how regulatory practices of the biometrics discourse govern culturally intelligible and acceptable notions of identity.
And related to that, in the biometrics discourse the bodily aspects become the ultimate decisive factor in determining who one is. What does this decontextualization imply for the acting

subject? As Lyon puts this issue: 'Body surveillance reduces identity questions to what can be found in the text of the body itself. It bypasses the acting subject, who may wish to explain herself, or to put things in a longer historical context, by appealing only to the speechless "truth" that DNA samples or hand scans can provide. It is data from the object of the body rather than speech from the acting subject that is to be relied on in the last analysis' [Lyon 2001: 306]. Biometrics seems to decontextualize people from their motivations and environments. The way the body is made legible then leads to a preoccupation with visible properties, and a suspicion, or exclusion, of tactile properties that lie beyond the scope of biometrics. This can be a particularly questionable practice when it is related to biometric body surveillance, since many social problems have socio-economic contexts: people may have good reasons to act in a certain, unaccepted way. Body surveillance basically ignores this, by focusing mainly on behavioral aspects. One could even speak of a 'new behaviorism' here, because it first and foremost aims at describing physically perceptible aspects, instead of psychological motivations [Lyon 2001: 306]. The same point can be made when looking at the effects of camera surveillance such as practised with Closed Circuit Television (CCTV). CCTV is only focusing on acts, not on motivations people have for acting in certain ways, thereby taking the acts out of the context of the situation. Socio-economic problems are reconceptualized in terms of visible behaviour, just as biometrics reduces identity to what can be found in the text of the body, instead of conceptualizing them in terms of motivation, thus hiding the actual causes of problems and thereby conforming to the status quo.

So, when a shift is made from paper files and documents to body surveillance, we come to rely more and more on data images. What does this mean for the way we see and identify each other and ourselves as human beings? How is our concept of identity and agency changed?

6. Conclusion

As has become clear in the previous part, dataveillance techniques have a constitutive effect on the ways in which we perceive of ourselves. Our physical presence is never naturally given and never neutral. Consequently, privacy cannot be based on a biologically given, or some sort of stable, authentical core to be found within the body. It hereby loses its alleged stability. Consequently, there is no room left for the traditional notion of privacy as a gatekeeper that protects the subject from the outside world.

So we must ask ourselves: is there still a use for privacy in contemporary societies? To answer this we need to look at agency as it is changed due to the advent of new technologies. Think of digital information: there is no definite act of closure that can be performed on a digital file, it is always open to modification. This culminates in an ongoing proliferation of variants, and a continuous process of mutation of files that serve as source material. The flux of digital information can never be fully contained. It can only be followed.

Dataveillance is implemented in order to enable this following. Although the latter is more and more extensively used in contemporary societies, it remains impossible to pin subjects down. It becomes increasingly more difficult to get a grip on subjects when they engage in virtual communication. Therefore the desire to completely articulate and formalize the behaviour of subjects remains an *impossible ideal of power*, since it is based on the idea of a closed world that can be completely calculated and made predictable.

So instead of, on the one hand, adopting a pessimistic view of technology where we treat it as an evil that threatens the supposed integrity of our human subjectivity, or, on the other, celebrating privacy as an unconditionally given safe haven from which we can judge supposedly privacy intruding technologies, we are left in an in-between position.

Exactly such an in-between position has been the role of privacy: intermediating between dichotomous spheres, protecting the one from intrusion by the other, offering a form of resistance for the subject.

Why should we keep privacy as a valuable concept, now that we have revealed its dependency on specific, contingent power structures? Privacy has mainly served a protective role: to protect the private sphere from the public sphere, to offer a form of resistance against the intrusion of the outside world on the bare subject. This protective function is something we might want to adhere to. We are however not attempting to give a new meaning to privacy, which would result in exactly that ontological predetermination of privacy from which we have been trying to get away. We should not strive to fill in the emptiness that we ourselves have left behind. However, an alternative notion of privacy that may be salvaged is one of privacy as a *dynamic evaluative concept*. Privacy here emerges as the ability to engage in critical elaborations: the human subject may reflect upon its dependence on existing power structures. As there are no pre-set structures that proactively set standards for the use of privacy, it should in our view be seen fundamentally contingent over time, and permanently needs to be worked upon. So, the in-between position is not something to be afraid of, it restores a creative potential at the level of the subject which may grant new possibilities. We should neither be fearful of technology, nor should we be hopeful of privacy as being a safe bastion that will protect our true selves: 'There is no need to fear or hope, but only to look for new weapons' [Deleuze 1997: 309].

References

Butler, J. (1999), Gender Trouble: Feminism and the Subversion of Identity, Routledge

Deleuze, G. (1997), 'Postscript on the Societies of Control', in Leach, N. (ed), Rethinking Architecture: A Reader in Cultural Theory, Routledge

Foucault, M. (1972), The Archaeology of Knowledge, Pantheon

Foucault, M. (1979), Discipline and Punish: The Birth of the Prison, Pantheon

Gutwirth, S. (1988), Privacyvrijheid!: De Vrijheid om Zichzelf te Zijn, Cramwinckel

Haraway, D. (1991), Simians, Cyborgs and Women: The Reinvention of Nature, Routledge

Lyon, D. (2001), 'Under My Skin: from Identification Papers to Body Surveillance', in Caplan, J. and Torpey, J. (ed), Documenting Individual Identity: The Development of State Practices in the Modern World, Princeton University Press

Pateman, C. (1983), 'Feminist Critiques of the Public/Private Dichotomy', in Benn, S.I. and Gaus, G.F. (ed), Public and Private in Social Life, St. Martin's Press

Rodowick, D.N. (2001), Reading the Figural, or, Philosophy After the New Media, Duke University Press

Young, I.M. (1990), Justice and the Politics of Difference, Princeton University Press