Ascribing Moral Status to Personal Information

Informational Privacy for Individuals of a Digital Age

Ruth Elisabeth Martol Hansen

Master Thesis in Philosophy, Department of Philosophy, Classics, History of Art and Ideas

Supervisor: Reidar K. Maliks

UNIVERSITY OF OSLO

Spring 2014

Ascribing Moral Status to Personal Information

Informational Privacy for Individuals of a Digital Age

2014

Ascribing Moral Status to Personal Information: Informational Privacy for Individuals of a Digital Age

Author: Ruth E. Martol Hansen

http://www.duo.uio.no

Print: Reprosentralen, Universitetet i Oslo

IV

Abstract

The aim of this master's thesis is to present an argument for basing the moral value of informational privacy on an informational concept of personhood. Conventional liberal accounts of privacy, basing the moral value of informational privacy solely on the value of autonomy, will be shown insufficient in providing adequate rights to informational privacy in a digital age. I argue that in order to ascribe moral status to personal information, and through this status, informational privacy rights to individuals within the digital informational environment, the moral value of informational privacy must be based on the *direct* value of personal information. That is, rights to informational privacy are to be based on the constitutive role of personal information in making up and sustaining the informational person.

Acknowledgements

I am grateful to my supervisor Reidar K. Maliks who has given invaluable advice and helpful criticism; to my sister Christine Martol Hansen for proof reading and commenting on one of the last drafts; and to my parents Else and Ragnvald Hansen for their support.

Table of Contents

1 Introduction

This thesis considers the moral foundation for informational privacy rights. I will argue that developments in Information and Communication Technologies (ICT) have left the traditional liberal conception of personhood (as autonomy) inadequate in generating rights to informational privacy that are sufficient in providing protection of personal information in an age of digitalization. Rather than basing rights to informational privacy solely on a conception of persons as self-determined, autonomous agents, by virtue of which the individual is entitled to a normative ability to control access to her own personal information; I will argue that what is required for robust informational privacy rights, is a concept of personhood that recognizes the informational nature of persons to the effect of establishing the *direct* value of personal information. By establishing the direct value of personal information, the moral status ascribed to persons will be extended to personal information and *personal information* as such has a claim on others' respect. This in turn, places moral constraints on behaviour towards personal information.

Accounts of privacy have been many, various, and rivalrous. The liberal account of privacy is intuitive. Here traditionally, the individual's moral claim to privacy is based on the fundamental value of the autonomy of the individual. According to this view, rights to privacy are the individual's right to control others' access to herself. The liberal conception of privacy arises from a conception of the person as an autonomous agent, originating from the Cartesian world-view, according to which "no one can really know the thoughts and feelings of another person" (Alfino and Mayes, 2003 p. 11). By this account I have a direct knowledge of what is in and on my own mind, whereas others can only have knowledge about what is in or on my mind indirectly, that is, by me providing others with the relevant information. What is being assumed is the subject's privileged (epistemic) position when it comes to knowing the content of her own mind. That is, we are granted first-person authority when it comes to our own self-knowledge (McGeer, 1996, pp. 483-484). This essential first-person authority (or inscrutability) guarantees our individuality and our immunity to control by others (Alfino and Mayes, 2003 p. 11). Thus, in the liberal tradition, the person's right to control others' access to herself, or in other words, the person's right to privacy, is typically justified in terms of her nature as an autonomous agent. Privacy is taken as protecting the condition or property of being a person (Solove, 2009, pp. 29-30), and the value of privacy "[…] consist(s) of adhering to a moral duty to respect each individual's dignity and autonomy" (Solove, 2009, p. 85). Rössler for instance, suggests that "[s]omething is private if

one can oneself control access to this 'something'" (Rössler, 2005, p. 8), and privacy is important because it protects the autonomy of the person (Rössler, 2005).

Since it is common to distinguish between three kinds of privacy:

(i) Physical privacy = $_{def.}$ S' freedom from sensory interference or intrusion, achieved thanks to a restriction on others' ability to have bodily interactions with S. (Floridi, 1999, p. 52).

(ii) Decisional privacy = $_{def.}$ S' freedom from procedural interference or intrusion, achieved thanks to the exclusion of others from decisions (concerning e.g. education, health care, career, work, marriage, faith) taken by S and S' group of intimates (Floridi, 1999, p. 52).

(iii) Informational privacy = $_{def.}$ S' freedom from epistemic interference or intrusion, achieved thanks to a restriction on facts about S that are unknown or unknowable (Floridi, 1999, p. 52);

it will be appropriate, in this thesis, to limit the discussion to *informational privacy*, since the concern is the impact on informational privacy of the individual by new ICTs.

According to Benn (1988, p. 288) informational privacy, i.e. having control over access to personal information, is important in order to protect autonomy in one's self-presentation. That is, violations of informational privacy will "[…] impair one's capacity to manage the complex system of appearances with which one confronts the world" (Benn, 1988, p. 288). Similarly, Rössler (2005, p. 116) argues that informational privacy is important because having control over how we present ourselves to others is an intrinsic element in conceiving ourselves as autonomous individuals. Personal information is accordingly worthy of protection in contexts where unauthorized external access to such information jeopardizes the autonomy in self-presentation of the person in question (Rössler, 2005, pp. 124-125).

Concern about informational privacy has a tendency to emerge when assessing problems involved in or arising from changes in human interaction and communication patterns, such as those caused by developments in ICTs. For instance, one of the early

definitions of privacy[1] as "the right to be let alone" was expressed due to concerns about technological developments that threatened to cause disruptions of established patterns of communication and interaction. In 1890 Warren and Brandeis stated that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the predication that "what is whispered in the closet shall be proclaimed from the housetops"" (Warren and Brandeis, 1984, p. 76). This technological development has now developed into what, of some at least, is considered an information revolution. Solove, for instance, points to an "information revolution" that he describes in terms of a […] dramatic transformation of the way we shop, bank, and go about our daily business–changes that have resulted in an unprecedented proliferation of records and data" (2004, p. 1). Privacy concerns are no longer foremost that of having one's intimate personal information "proclaimed from the rooftops", but that of having "[…] the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own [preserved in] the collective computer networks of the world" (Solove, 2004, p. 1, my insertion), to the effect of digital "copies" or reconstructions of the "natural" person being created and manipulated by external parties in order to serve their particular interests.

The "information revolution" is taken a step further with the emergence of ubiquitous computing where the "digital" person is no longer only a digital reconstruction of a person's life, but the "natural" person is digitalized and incorporated into a computer network. According to Conti, et al., by ubiquitous or pervasive computing "[…] real-world components interact with cyberspace via sensing, computing and communication elements, thus driving towards what is called the *Cyber–Physical World* (CPW) convergence" (2012, p. 2, italics in the original). This means that the "natural" (i.e. "physical" or "concrete") person can be integrated in a computer network by virtue of (personal) information being seamless transferred into a digital informational environment where this information is "[…] elaborated to adapt cyber applications and services to the physical context […]" (Conti, et al., 2012, p. 2). With the CPW convergence 'things' become active participants in information processes, and by exchanging data and information sensed about the environment, they can communicate with each other and the environment, react independently to the communicated information, and influence it by running processes that trigger action with or without human

[1] Warren and Brandeis in *The Right to Privacy: The Implicit Made Explicit* (1984) tie the value of privacy with the individual's "right to be left alone" (Warren and Brandeis, 1890, in Schoeman, 1984, p. 14).

intervention (Gubbi, et al., 2013, p. 1647). For instance, a person with a heart disease can be fitted with an electronic cardiac device, such as a wireless implantable cardioverter-defibrillator (ICD). Such a device can store and communicate information of the patient's heart rhythm to medical staff so that they in turn can adjust the device accordingly in order to treat potentially fatal heart rhythms. However, by integrating the patient by means of the wireless ICD into a computer network, the patient is vulnerable to external improper modifications or manipulations in that unauthorized external parties could wirelessly communicate with the ICD to modify its settings and by this, not only gain knowledge of personal information, but cause the devise to issue a large shock (Denning et al, 2010, pp. 917-918). By this, the person itself can be altered or manipulated improperly by external information processing powers. Any inhabitants (or entities) integrated into such an environment are thus (sets of) information that can be operated on by information processing powers, leaving the person, like any other entity, constitutively made up of (personal) information.

The concern of this thesis is that this constitutive role of personal information is not reflected in traditional liberal accounts of informational privacy. Traditional liberal accounts consider personal information as knowledge about the particular person in question, the right to informational privacy is the individual's right to control others' knowledge about herself in contexts where such knowledge undermines her autonomy in self-presentation. By this, personal information is indirectly valuable on the condition of the value of autonomy, personal information as such having no particular moral value.

Traditional liberal accounts of privacy have been critiqued in various ways. Schoeman (1992), for instance, objects to basing the value of privacy on autonomy. He argue that autonomy suggests isolation, leaving privacy as "restrictions on others' access to a person," whereas privacy suggests involvement and intimacy, and enables individuals to form deep and meaningful relationships with family and friends. It is this associational aspect, according to Schoeman, that should be taken as the source of its value (1992, pp. 156-157). In this thesis the intention is not to reject the liberal concept of privacy on grounds that it is anti-associational, neither is it to question the value of autonomy as such, it is rather to express a concern over the value of autonomy as insufficient in providing needed restrictions on others' access to a person in a technologically advanced world.

I will argue that by conceiving the person as information, the information that is to be considered as worthy of protection by informational privacy rights is not to be determined on

condition of autonomy but by its constitutive role. By virtue of its constitutive role, personal information has direct value in relation to what it is constitutive of, that is, it has a direct value in relation to the set of which it is a member. Or, put differently, personal information is of direct value to the person it is a constitutive part of. By recognizing the direct value of personal information, by recognizing its constitutive role, the moral value ascribed the "natural" person can be extended to personal information. By this, the value of informational privacy is not to be considered as consisting in adhering to a moral duty to respect each individual's autonomy, but as consisting in adhering to a moral duty to respect personal information as such. I will claim that an informational conception of personhood will provide individuals with more robust rights to informational privacy, within a (digital) environment where both the entities inhabiting it and their patterns of interaction and communication are drastically different from those upon which the liberal theories traditionally are based, and the person's ability to control access is in effect limited to a choice in whether or not to partake in digital living (to the degree this is a choice).

In the next chapter I will first introduce the theories of Benn (1988) and Rössler (2005), that I take as representative of the traditional liberal conception of privacy, defining privacy rights as protection of autonomy. I will then discuss some difficulties facing these theories in relation to developments in Information and Communication Technology (ICT). In Chapter 3, as a preliminary for determining the moral criterion for informational privacy rights, I will give an outline of Floridi's (2011) account of the informational person, introduce the person as a unique set of information and suggest personhood as a particular degree of informational detachment. In Chapter 4, I will develop the moral criterion for informational privacy rights. I will argue for extending the moral status ascribed the "natural" person to the informational person to the effect of attributing moral status to personal information. I will defend the direct moral value of personal information as the criterion for informational privacy rights.

2 Privacy and the Liberal Conception of Personhood as Autonomy

As mentioned in Chapter 1, in thesis I will argue that by our extensive adoption of new ICTs (developed by computer scientists and engineers), the ways in which we interact will be subject to fundamental changes to the effect of a need for a re-conceptualization of who we are. When such a re-conceptualization is in place, a new account of the moral value of personal information, one that will generate more adequate informational privacy rights, will be available. In preparation for such an account I will in this chapter consider two influential liberal theories on privacy that I take as representative of the prevalent or common (liberal) views on privacy and privacy rights, namely those of Benn (1988) and Rössler (2005). I will in the following section give an outline of these two theories, then, in section 2.2 I will turn my focus to informational privacy, and I will touch upon some problems faced by theories that conceive of personhood in terms of autonomy when arguing for the right to informational privacy (this will also be further discussed in later chapters).

2.1 The Traditional Liberal Conception of the Value of Privacy

In this section I will give an outline of the liberal theories of privacy of Benn (1988) and Rössler (2005) as a foundation for the upcoming discussion. I have chosen these theories because they are in line with the view I initially intended to defend, namely that rights to privacy are due us because of our nature as autonomous, self-determined agents. Benn (1988) argues that privacy is necessary in order to respect persons as choosers. Rössler (2005), on the other hand, argues that we value privacy because we value autonomy, that is, without the protection of privacy, a life led autonomously would not be possible. Although Rössler (2005, p. 71) accuses Benn (1988) of becoming reductive in his approach to privacy, this debate is not of concern here, what is essential is that they both base privacy, in some way or other, on the value of autonomy. I have included both in order to enrich the argument in the following chapters. I will begin by giving an introduction of Benn's (1988) view on privacy and then turn to Rössler (2005).

According to Benn, since a person knows himself as thinking and feeling, and

because this consciousness of inwards processes itself can be the intentional object of thought and feeling, to be conscious of oneself as a natural person is to believe that one's conscious processes are causally effective, that is, to believe that what makes the difference to the world is one's deciding (Benn, 1988, p. 92). This means, according to Benn, that "[t]he actions of a person are the effects of his having beliefs and recognizing, even if sometimes inadequately, what they commit him to do" (Benn, 1988, p. 92). For someone to be a natural person is, accordingly, to be aware of oneself as a decision maker or chooser whose decisions can make a change to how the world goes (Benn, 1988, pp. 90-94).

By recognizing oneself as a chooser or a natural person (that is by seeing oneself as a project maker) in a world with others like oneself, a conception of oneself as a moral person is developed. By being conceptually equipped to grasp what it is to have and value projects of his own, a natural person is thereby committed to respecting every other person as an originator of projects. By claiming respect, that is, the recognition of our moral personality on the grounds of our natural personality, we are committed to extending it to anyone else satisfying the same conditions (Benn, 1988, p. 94-99). This principle of respect presupposes a certain minimal equality since "[…] it is grounded in the fact that each speaks from his own particular point of view, having perceived interests that no one else can presume to know in advance of inquiry, and which cannot be assumed to be interchangeable with anyone else's" (Benn, 1988, pp. 104-105). Respect for persons is therefore due to all persons alike, and is "[…] to see him as a subject for a principle of equal consideration of interests […]" (Benn, 1988, p. 106). The relating interests are, not only the things that would be, or believed by the person to be, to his advantage, but also the elements that form the person's identity over time in that they are the forms of activities that he perceives as giving points to his actions and projects. Through his identity of interests the person is then able to see continuity of meaning and pattern in what he is and does (Benn, 1988, pp. 106-107).

> His projects are an exteriorization of himself, projections, indeed, of himself into the world; his identity as a person […] depends on his sense that they are indeed his own, informed by interests which together constitute him an intentional agent with an enduring nature, not simply as a stream of experiences, even of remembered and envisaged experiences" (Benn, 1988, p. 107).

We have a moral claim to privacy, according to Benn, because others' observations or scrutiny of us has impact on our decision-making. By being observed, that is, by finding himself as the focus of the observer's attention, the agent will change his perception of his

own actions in that the agent will see his actions through the eyes of the observer (Benn, 1988, pp. 272-273). Accordingly, Benn views the normative aspect or dimension of privacy as respect for individuals as choosers:

> I am suggesting that a general principle of privacy might be grounded on the more general principle of respect for persons […] To *conceive* someone as a person is to see him as actually or potentially a chooser, as one attempting to steer his own course through the world, adjusting his behavior as his appreciation of the world changes, and correcting course as he perceives his errors. […] To *respect* someone as a person is to concede that one ought to take account of the way in which his enterprise might be affected by one's own decisions. By the principle of respect for persons, then, I mean the principle that every human being, insofar as he is qualified as a person, is entitled to this minimal degree of consideration (Benn, 1984, pp. 228-229, italics in the original).

The moral claim to privacy, however, seems to cause tension in relation to the liberal *principle of non-interference.* This principle arises from assuming that the rationality conditions that a decision maker must satisfy in order to be considered a subject for respect, are satisfied if the person is capable of assessing possible courses of action in terms of their outcomes, weighing cost against benefits, and of arriving at a decision on the basis of an ordered set of preferences, and, of forming his beliefs on evidence and to suit his actions to his beliefs. When, however, a person is made un-free to act these conditions are usually affected, actually or possibly, by someone's interference (Benn, 1988, pp. 152-154). The *principle of non-interference* thus ascribes "[…] a general liberty to do whatever one chooses unless someone else has good grounds to interfere to prevent it, grounds that would appeal to any rational person" (Benn, 1988, p. 271), The burdens of justification by this principle will always fall on the interferer, not on the person interfered with (Benn, 1988, p. 87). Privacy rights, as rights to limit or control others' access to physical, mental, or informational spheres, initially seem contradictory to the principle of non-interference. Privacy claims will restrain the observer's action of observing, and by that interfere with the observer's liberty to do whatever he chooses. In the case of privacy violations, however, the observer will, by his mere *presence,* restrain the agent's actions, to the effect that the observer has violated the agent's status as a chooser (that is, his status as a natural and moral person). By this violation, the agent (the observed) will have a moral claim, on the observer, of immunity to observation if the agent satisfies the conditions for natural personhood. Benn, therefore, argues that the certain basic features of our conception of a person requires some minimal right to immunity from uninvited observation and reporting (Benn, 1984, p. 224). In noting that privacy

amounts to respect for persons as choosers, Benn takes it that privacy protects personhood because observation (or surveillance) restricts an individual's range of choices to the effect of a limitation on the individual's freedom (Solove, 2009, p. 30).

According to Rössler, a person would not be described as free if she acted in the pure freedom of the chooser, making her choices 'only' freely, arbitrarily, without reason. Her choices must be grounded or determined by a certain attitude towards herself and towards possible options. This attitude is the attitude that the person has toward her own life or life projects. The person must therefore be able to ask herself the "practical question" relating to how she would like to live, what sort of person she wants to be, and how she should best strive for her own good in her own way. The capability to ask and follow through the practical question presupposes freedom, but this kind of freedom requires personal autonomy. According to Rössler, it is a fact that a life led autonomously seems 'more valuable' than a merely free life (i.e. an unconsidered life) and this is why we expect autonomy from persons in their actions. The possibility of asking ourselves the practical question, however, can be understood as the extent to which we have the possibility to distance ourselves somehow from our desires, the roles in which we find ourselves, and our guiding norms, and ask what oneself is in all this, and what it is that I myself want? And this results, in Rössler's view, in the possibility of behaving reflectively with respect to one's own life. Personal autonomy is, accordingly, general personal self-determination concerning how one wants to lead one's life. What makes general personal self-determination or the autonomously led life possible, is the moral respect for a person's autonomy. Individual personal autonomy is therefore, according to Rössler, only possible within a social network which recognises and acknowledges moral norms such as respect, fairness and tolerance (Rössler, 2005, pp. 49-51).

To be self-determined or autonomous, according to Rössler, means that the person can identify with her desires and actions as her own. This amounts to her desires and actions being authentically hers. In order for this to be, she must be able, and be in a position to reflect upon her desires, and by such reflection decide on whether to accept, reject or modify them. Authenticity is expressed in terms of "evaluative identification" as opposed to "confirmatory identification" (Rössler, 2005, p. 53). The goal of *evaluative identification* is "[…] to be able to choose between different desires, possible modes of behaviour and ways of life in such a way that an autonomous decision is the result" (Rössler, 2005, p. 53). This means that if a person's actions were to be exclusively guided by convention and other persons' preferences, without any evaluations of her own, she would not be considered

autonomous (Rössler, 2005, p. 53). I take it that confirmatory identification, on the other hand, would be when a person accepts and identifies with any desire whatsoever, the person would identify or confirm the desire as her own, but this identification would not be based upon a critical process which is a condition for autonomy (Rössler, 2005, p. 54).

Because the process of reflection and identification will always incorporate personal obligations, feelings, memories, and biographical influences, a person's reasons for identifying "good reasons", need not seem like good reasons to other people, it would therefore, in Rössler's view, be inappropriate to bind autonomy to a strong notion of rationality. A person is autonomous, when she has her own good reasons for identifying with certain desires and rejecting others, when she is able to understand herself as the author of that action (this, however, need not mean that other people also accept these reasons). A person must also be guided by true opinions about the world and her relations to other persons, and by true, valid opinions about herself, her own abilities and her own history. According to Rössler, because there is a historical component in the concept of autonomy, a desire could come about as a product of manipulation even though the desire fulfils the requirements of authenticity. This means that authentic identification is not always or necessarily sufficient to show the person in question as genuinely autonomous. It is therefore necessary to reflect on the genesis of a desire or action, especially with respect to the person's individual capacity for developing a non-manipulative relationship towards herself, to decide on the authenticity of a respective desire or action. This means that reflection on what subjective context the desire or action was formed in, is necessary to prevent (as far as possible) self-deception and manipulations. Personal autonomy necessitates also non-manipulative outwards circumstances in that non-manipulative social relations allow the person to build upon forms of recognition that are intrinsic to the development of a non-manipulative self-relationship (Rössler, 2005, pp. 54-61).

> A non-autonomous life in this *external* sense would thus be one that is lived under conditions that (necessarily) bring the person to form systematically false opinions – at least in certain respects – about her possibilities, actions, goals, desires and expectations, that is conditions of systematic repression, manipulation and deception (Rössler, 2005, p. 61).

A constituent element of the development of individual autonomy is therefore a social or relational element because persons are dependent on inter-subjective communication that conveys to them that their own self-identification or identity is taken seriously. Through this,

the person can gain self-respect (Rössler, 2005, p. 62). The degree of successful inter-subjective communication depends, however, on the way others are involved in one's affairs. How particular standpoints are involved in a communication or how their degree of involvement influences a person's self-perception (as an autonomous subject), how she acts and how she presents herself (Rössler, 2005, pp. 116-117). Because we are influenced by the presence of others, other's privacy should be respected when we realise that our behaviour may influence their self-perception and behaviour in undesired ways (Rössler, 2005, p. 117). Privacy has therefore, according to Rössler, the function of permitting and protecting autonomous lives in that "[r]espect for a person's privacy is respect for her as an autonomous subject" (2005, p. 117). Our reasons, according to Rössler, for wanting 'a room of our own' or for wanting to be able to control what others know about our private life is that

> To be able to ask oneself authentically why one is and how one would like to live, it is clearly necessary to have possibilities for withdrawing from the gaze of other people. To be able to conceive, develop and pursue goals, it is necessary to have dimensions in one's life that are free from the objections and control of other people. To be able to develop authentic plans, to design or define oneself through one's dealings with 'specified others' one's expectations with respect to other people's knowledge about oneself must not be mistaken (2005, p. 73).

Rössler claims the distinction between a public and private realm as constitutive because it expresses the fundamental notion of individual freedom and the autonomy of the person, her thesis being that "[…] the true realization of freedom, that is a life led autonomously, is only possible in conditions where privacy is protected" (2005, p. 72).

According to Rössler, in the liberal view of privacy, "[…] something is regarded as private if one can oneself control access to this 'something'" (2005, p. 71). On this notion of privacy the protection of privacy denotes protection from undesired access by others. By this, a person have a right, by virtue of her autonomy, to be able to control access to particular places (such as her room or home (Rössler, 2005, p. 71)), a right to control "[…] who has access in the form of opportunities to intervene or intrude in decisions relevant to the person herself or in actions not directly concerning others" (Rössler, 2005, p. 71), as well as having a right to have control over who has access to which knowledge about herself, i.e. control over who knows what *(relevant)* data about her (Rössler, 2005, p. 71). As mentioned in Chapter 1, this thesis will concern this last kind of privacy rights, that is, with individuals' rights to informational privacy.

2.2 Informational Privacy, Self-Knowledge and Autonomy

In this section I will account for informational privacy in relation to the value of autonomy. I will briefly consider some difficulties facing the liberal accounts of informational privacy, and (although somewhat superficially) argue that by basing their accounts on autonomy to the effect of generating control rights to informational privacy, they neither capture the severity of informational privacy violations, nor are they sufficient in view of evolving technologies. I will then anticipate a solution that involves a unification of the person with her information that will allow the moral status ascribed the former to be extended to include the latter.

Benn's view on informational privacy is that a person should be able to "[…] prevent unauthorized access to facts about oneself that 'give one away' – that if freely available would impair one's capacity to manage the complex system of appearances with which one confronts the world" (Benn, 1988, p. 288). According to Benn, when publicized, private information will have a tendency to be fixed as public, objective facts, and this forces us to see ourselves as others see us. This, however, does not necessarily make us see ourselves more truly, but it may, nevertheless, alter our own self-perception: "[…] the eye of the *voyeur* can impose its soiled vision on the self-consciousness of its object, to affront and spoil what it sees" (Benn, 1988, p. 288, original italics). We should therefore be able to control access to such information.

Informational privacy, according to Rössler, implies limits to knowledge. "If privacy in general means being *able* to control 'access' to one's personhood, then […] this must in one respect be understood and interpreted as control over what other people can *know* about oneself" (2005, p. 111, italics in the original). According to Rössler, 'control' means control over who knows what about a person and how they know it, i.e. " control of the information relating to that person" (2005, p. 111). Similarly to Benn, Rössler argues that informational privacy matters to us because we see it as an intrinsic part of our self- understanding, as autonomous or self-determinate (autarchic[2] or self-directing in Benn's terms) individuals, to

[2] On Benn's account, being autarchic is to be a decision-making subject, satisfying the minimum conditions of rationality mentioned above. Autarchy is thus "the normal state of the natural person" (Benn, 1988, p. 184). To be autonomous, on the other hand, is "to live according to a law that one prescribes to oneself" (Benn, 1988, p. 155), and goes beyond autarchy in that autonomy is an ideal for the autarchic person to strive for and which can be achieved in varying degrees. According to Benn, however, a human being is not defective either as a human or as a person because of falling short of autonomy, only by falling short of autarchy is a human being considered defective as a human or person (Benn, 1988, pp. 154-155).

have control over our self-presentation. According to Rössler, if we lose the ability to control how we want to present or stage ourselves and to whom and in which contexts we want to do so, we would no longer be able to regulate the range of our diverse social relations. Without self-determined control over what one allows to be known about oneself and by whom this information about oneself is to be known, neither self-determined, context-dependent, or authentic behaviour would be possible, nor would one be able to authentically (or autonomously) find an answer to the practical question (Rössler, 2005, p. 116). This is because

> [t]he very moment the deceived person becomes aware of the situation, the presence of observers, the knowledge of unexpected third parties, or the deception on the part of actual communication partners always results in a change or shift in perspective. And it is just such an involuntary shift in perspective from the first to the third person that prevents self-determined, authentic behaviour […] (Rössler, 2005, p. 116).

As previously mentioned, traditional liberal theories of privacy as protection of autonomy originate from the internalistic (Cartesian) view of the mind, which is that "no one can really know the thoughts and feelings of another person, that is, we have first-person authority when it comes to our own self-knowledge. This essential inscrutability, which was supposed to guarantee our individuality or identity and our immunity to control by others, must, however - with the realization that there is no metaphysical boundary between mind and body, we are prone to others knowing and (to some extent) controlling our thoughts and feelings - be rejected on philosophical and scientific grounds. (Alfino and Mayes, 2003, p.11-12). Ryle, for instance argued that:

> The superiority of the speaker's knowledge of what he's doing over that of the listener does not indicate that he has privileged access to facts of a type inevitable inaccessible to the listener, but only that he is in a very good position to know what the listener is often in a very poor position to know (1984, pp. 155-156).

McGeer seems to think that, although we might gain information about ourselves by different means than the means by which others gain information about us, the information we and others gain about ourselves are of the same kind, the difference being that of amount. We have first-person authority over ourselves because our judgements about ourselves are based on more of the same kind of information available to others (McGeer, 1996, p. 500). However, in regards to informational privacy and new technology we might risk loosing our superior position to view and judge our lives; our first-person authority might be under siege.

Information we used to assume unknowable to others might easily, by (new) technology, become freely available. Wasserstrom (1984, pp. 325-326) argues that the consequences of the availability and easy access of enormous amounts of information about each of the individual members of a society provided by technology could enable others with a picture of one's actions that is "[…] fantastically more detailed, accurate, and complete than the one I could supply from my own memory […]" (Wasserstrom, 1984, pp. 326). This scenario emerges as a realistic picture through the concept of a life-log, where a person's life is being digitally chronicled by a continuous, detailed recording of every aspect of that person's life (Allen, 2011, pp. 165-171.) Since our capacities for gathering, processing, and storing information is limited (Manders-Huits, 2010, p. 44) the amount of information in a life-log would be greater than the sum of information that would be possible to store in the "analogue" memory of a person (human being). This would mean that something or someone other than the person, whose life is logged, might be in a better position than herself to make judgements about her (depending on who has access to the life-log).

This can be further exemplified in terms of what James (1892, in Lieberman, 2012, p. 67) viewed as, the two components of the self: the *I* and the *ME*, according to which, the self can be viewed as "[…] an objective person, known by a passing subjective thought and recognized as continuing in time" (James, 1892, quoted in Lieberman, 2012, p. 67). Self-knowledge can be viewed, according to Lieberman, as a special file cabinet called *ME*. The *I* is the active part of the self: it fills the file cabinet and can later peruse its content (Lieberman, 2012, p. 67). When the file cabinet or the *ME* is understood as personal information and the *I* as the autonomous, authentic agent (in terms of Rössler) or (in Benn's terms) the "natural" person, then, in light of the above argument of new ICTs, something other than the *I* could easily be in possession of a greater "*ME*– file cabinet" than the *I* that fills it, and privileged self-knowledge is no longer obvious.

The important point to be drawn from the above is that our superior position or privileged access to our own "file cabinets" is an essential condition for personal identity. If we are no longer guaranteed a superior position or privileged access to our own *ME*s, that is, to our own personal information, a moral right to informational privacy should afford such a superior position or privileged access. I do not think, however, that the conception of autonomy as personhood is sufficient to provide informational privacy rights that are sufficiently robust to secure our privileged access to our own personal information.

As mentioned above, life-logging is the continuous monitoring or recording of a

person's contextual activity, "[…] where a person utilizes passive capture devices to record and digitalize his life" (Hernandez, et al., 2013, p. 234). In life-logging the person uses a wearable computer that for instance, can, by biosensors, monitor physiological changes of the user, and, for example, by a mobile-phone camera, can collect images from the perspective of the user in order to capture the events leading up to the physiological changes. The data can be transmitted over the Internet and Bluetooth to provide both the user and others with access to otherwise more or less inaccessible information of the user (Hernandez, et al., 2013). Life-logging has potential to serve many purposes especially healthcare related purposes. For example:

> […] some of the most prevalent and disruptive symptoms of Autism Spectrum Disorders (ASD) include stressful challenging behaviors (e.g., self-injury, repetitive behaviors) and impaired verbal communication. If teachers, therapists or family members could also have access to information of the internal state of people with ASD, they could potentially gain deeper understanding of the emotional states of the individual and prevent the occurrence of challenging behaviour […] long term physiological information could also be helpful to doctors so they can better assess the symptoms of their patients and make better diagnosis of chronic conditions (e.g., epilepsy, anxiety-disorders, depression) (Hernandez, et al., 2013, pp. 326-327).

According to Hernandez, et al., the privacy of the user is maintained by the camera being easy to switch on and off, in order for the user to determine which situations data should or should not be captured (2013, p. 326). The user is thus provided with the ability to control others' access to her information. When the user decides to leave the device on, however, the user has little control over how her information is being handled or used. How her data is being stored and to whom it is transmitted is not in the hands of the user but in the hands of those who designed or engineered the system[3]. When it comes to the above example, on the other hand, some people with autism might not even be able to control the off switch, and would thus have no means to control access[4]. Thus, it is not at all obvious that theories that are basing informational privacy rights on autonomy that in turn generates control rights to informational privacy, are sufficient in view of the challenges to informational privacy of the individual posed by new technology.

Implicit in any account of privacy that justifies informational privacy in terms of

---

[3] The impact new ICTs have on our ability to control access to and use of our own personal information will be discussed in section 4.1.

[4] According to Benn (1988, p. 94), however, such a person might not qualify as right holders of informational privacy, this will be briefly discussed shortly.

autonomy to the effect of informational privacy rights being rights to control access to personal information, is, in my opinion, a division between personal information and the "person". When informational privacy is considered as *control* rights, informational privacy seems to entail ownership, that is, personal information seems to be considered only as a product produced by the agent, and therefore his to own and consume. Moore, however, points out that, since personal information can be copied, personal information, can also be non-rivalrously consumed. A person's right to control information about himself also does not exclude the possibility of others also owning such information[5] (Moore, 2010, pp. 84-87). Concerns about informational privacy is thus not centred round the value of personal information as such in relation to its originator, but centred round the person's normative ability to control particularly valued spheres. Theories of informational privacy based on one's right to *control* information about oneself, can thus only compare privacy violations to trespassing or unauthorized intrusion of a "[s]pace or sphere of personal information, whose accessibility and usage ought to be […] controlled by its owner and hence kept private" (Floridi, 2005, p. 193). By comparing privacy violations to trespassing, control-based theories do not seem adequate in order to account for the severity of the distress caused by (at least some) violations of informational privacy. On the other hand, as stated by Floridi

> "[m]y" in "my information" is not the same "my" as in "my car" but rather "my" as in "my body" or "my feelings": it expresses a sense of constitutive *belonging,* not of external *ownership*, a sense in which my body, my feelings and my information are part of me but are not my (legal) possessions (2005, p. 195, italics in the original).

When personal information is considered not only as something *produced* by the person, but, as an essential part of the person herself, one will realize that – as one would not consider the unauthorized removal of someone's leg as mere theft, but as that of causing physical harm to the person in question – when a person's personal informational is accessed without authorization, it should not be considered merely as a violation of this person's normative ability to control access to a particularly valued sphere of her personal information, but as that of causing *informational harm* to the person (since such access endangers her stable

---

[5] Moore's solution to this is by employing a version of John Locke's proviso on acquisition: "For this labor being the unquestionable property of the laborer, no man but he can have a right to what that is once joined to, at least where there is enough and as good left for others*"* (Locke, 1980 [1689], quoted in Moore, 2010, p. 84). When *enough and as good* is viewed as a "no harm no foul rule" or in Moore's terms as a Pareto-based proviso, actions that pass this standard would leave little room for rational complain (Moore, 2010, p. 84). Informational privacy rights are justified in that the individual's use and control over their own personal information would not necessarily worsen others (Moore, 2010, p. 85).

functioning as an autonomous informational system[6]).

In relation to the above example of life-logging and wearable devices, I think it appropriate to point out that an informational re-conceptualization of personhood would provide an answer to another point of concern for the liberal accounts of informational privacy. According to Benn "[i]t is the fact of natural personality, not of humanity, which makes the crucial difference between right bearers and other objects" (1988, p. 240). Although Benn makes allowance for someone defective in autarchy to qualify as a person, "[t]he respect that is owed to a person may generate different rights and immunities where the person is nonautarchic" (1988, p. 156). This would mean that, because privacy rights are grounded in the *principle of respect for persons,* someone defective in autarchy (depending on their defect) would, at least to a certain degree, have limited moral rights to informational privacy. Similarly to Benn, Moore, although not accounting for privacy rights as the protection of some essential or intrinsic value of autonomy, argues for autonomy as a condition for acquiring (privacy) rights in the first place. Individuals acquire rights to control their own bodies, capacities, and powers gradually as they grow into adulthood, and they may fade away at the end of life (Moore, 2010, p. 64). The need for privacy is, according to Moore, due to the universal need for separation as part of securing survival. What distinguishes separation from privacy, on his account, is that rights entail obligations and claims against others, and it is the capacity of free will that caters for such obligations and claims. Because it is the subjects' capacity of free will and not the potential of free will that gives rise to privacy, privacy rights can only gradually be obtained in accordance with the development of the subjects' capacities. This means, according to Moore, that privacy rights come in degrees (Moore, 2010, pp. 47-64). Persons who have developed their capacity for rationality or free will to perfection, would be the ones entitled to the most comprehensive rights. On the other hand, some individuals may never be able to obtain privacy rights even to a minimal sufficient degree. On Rössler's account, we value privacy because privacy is that which enables autonomy. According to Rössler, it is only if privacy is protected, that a life led autonomously is possible (Rössler, 2005, p. 72). Whilst agreeing with Rössler that protection of privacy enables autonomy and that autonomy is important, I think Rössler is mistaken about autonomy as the sole grounds for valuing informational privacy. Not every human being can be considered autonomous, that is, not everyone is capable, in Rössler's

[6] This claim will be explained and defended in Chapter 4.

terms, of asking herself "the practical question". This does not, however, mean that informational privacy, for these people, should be considered without value, or that avoiding the harms that can accompany violations of informational privacy is without interest for "nonpersons". My claim is that, because (as it will become obvious) informational privacy rights should not be based on personhood as autonomy, but the more inclusive concept of informational personhood, any account ascribing informational privacy rights as a matter of degree would be unjustified.

Thus, in what to come, I will argue that the appropriate grounds for justification of informational privacy should neither be autonomy, authenticity, or autarchy, nor should the right to privacy be that of a right to control. I will argue that we must reject the view of a person's information as produced by that person and thus theirs to control, and instead suggest a unification of the person and her *personal* information. This means that personal information should be considered an essential part of, and therefore, not to be readily separated from, the person (whatever 'person' might mean). By considering personal information not only as a product of the *I* or the *person*, but instead fully incorporate information into the person or agent, personal information should be valued as essential or constitutive parts of ourselves. When (personal) information is viewed in this way, the moral status of the person should be extended to include her constitutive information, which will provide us with forceful rights to informational privacy.

In order to defend a view of informational privacy based on informational personhood, it will be necessary to explain the nature of informational selves.

3 Informational Conception of Personhood

In the previous chapter I implied that a unification of the person with its information is required for an adequate justification of informational privacy rights. Even though Benn and Rössler's liberal conception of personhood, in my view, initially seems to provide intuitive justifications for informational privacy rights, I find it lacking in its ability to provide for informational privacy within the informational environment (due to advances in information and communication technologies). The digital informational environment is made up of "[…] programs, algorithms, data structures, and other objects […]" (Colburn and Shute, 2010, p. 97) that are not subject to physical constraints (they are, however, subject to logical constraints) (Colburn and Shute, 2010, p. 97). Both the (interacting) informational entities and their patterns of interaction are constructed through new Information and Communication Technologies developed by computer scientists and engineers. Since we increasingly live our life in the environment they create, these technologies have great impact on our lives. In the digital world or environment the informational nature of the person becomes apparent in that "[d]igital technology enables the preservation of the minutia of […] who we are" (Solove, 2004, p. 1), That is, in the digital environment the person is a collection of data which is "[…] digitized into binary numerical form, which enables computers to store and manipulate it with unprecedented efficiency" (Solove, 2004, p. 2). The informational nature of the person, however, is not reflected in conception(s) of personhood, and so we do not recognize that when we are dealing with personal data or information in the digital world, what we are dealing with is the person itself. I will therefore argue that what is required for a sufficient justification of informational privacy rights in order to provide for informational privacy within the digital informational environment, is that the concept of personhood upon which these rights are to be based, must adequately reflect the informational nature of the person.

Thus, as a preliminary for determining the moral criterion for informational privacy rights (in Chapter 4), in this chapter and based on Floridi's (2011) construal of the person as a multi-agent system, I will argue for a conception of the person, as a set of information, that is, for an understanding of the person as constitutively made up of information and informational processes. Personal information is not, on this view, a product of the person in question, but rather the person itself.

As mentioned in section 2.1, Benn (1988) argues that the condition of personhood is to see or consider oneself as a chooser. A person knows herself as thinking and feeling; thinking and feeling are inward processes, and these inwards processes can themselves be the

intentional objects of thought and feeling. This implies that to be conscious of oneself as a person, that is, as a chooser, is to believe that these inward processes are causally effective (Benn, 1988, p. 92). A person's identity is, according to Benn, a "continuing identity of interests" (1988, p. 107). Interests are, in this context, to be understood as

> […] those forms of activity which provide the foci for his attention and which he perceives as giving point to his actions and his projects. They are those things in which he "takes an interest," such as the welfare of his family, his football team, music, philosophy, or the freedom from Hunger Campaign" [the person's interests] provide the strands of his identity over time, through which he is able to see continuity of meaning and pattern in what he is and does (Benn, 1988, pp. 106-107, my insertion).

By this, a person takes on a variety of interests, but since we are subject to a diverse range of competing possibilities, the coherence of a person's set of interests depends on being informed by the stable values and principles of the person in question. By stable values and principles she can place *herself* amongst the competing possibilities and recognize or create in herself a coherent set of beliefs to the effect of creating for herself a personal identity. Coherence or consistency is however something that can only be aimed at but not perfectly achieved. (Informational) privacy is, accordingly, justified by our need for being able to choose what to reveal of ourselves in different situations in order to establish, sustain, and develop our personal identities (Benn, 1988, p. 282). Informational privacy is thus, according to Benn, the ability to "[…] prevent unauthorized access to facts about oneself that "give one away" – that if freely available would impair one's capacity to manage the complex system of appearances with which one confronts the world" (Benn, 1988, p. 288).

Similarly, Rössler argues that informational privacy matters because we view it as an intrinsic part of our self-understanding as autonomous individuals to be able to control our self-presentation. In order to manage our self-presentation, we must be able to control access to our own personality. It should therefore, to a great extent, be in the hands of the person to control what others know about her, or at least the person should have the ability to guess what others know about her in any particular situation (Rössler, 2005, pp. 111-116).

According to Benn and Rössler, we have an interest in informational privacy because we consider ourselves as autonomous choosers or because we value autonomy. In these theories, informational privacy is considered only to involve a right to *self selected* self-presentations, justified by conceptions of persons as choosers or by the value we place on autonomy. Informational privacy rights are accordingly, rights to control or at least to

monitor what information about oneself is revealed or known by what others in which situations. Accordingly in these theories, what we are jeopardizing by violations of informational privacy is *only* our *self selected* self-presentations.

Contrary to this I will argue that within the informational environment, informational privacy is not to be considered as just involving a person's right to autonomy in her self-presentation, but a claim on others to treat personal information as moral entities[7]. The person is embedded, by rapidly evolving informational technologies, in "the informational environment" by virtue of her personal information. In order to fully appreciate the implications these technologies have on our interactions within the "informational world", as 'online (informational) agents' or 'networked persons', we need a new conception of what an online or networked person is and how (personal) information is related to such an agent or person. I suggest that, in this context, the appropriate conception of personhood is that of persons as appropriately enclosed sets of information and informational processes. I will argue that this conception of personhood will provide a stronger justification of informational privacy rights. When we conceptualize personhood in informational terms, that is, when a person can be conceptualized as constitutively made of information, unauthorized access and distribution of personal information would not just impair one's capacity to manage a system of appearance, or self-presentation, but unauthorized access and distribution would impair the (informational) person herself. In informational terms, taking or collecting, and distributing personal information is not to be considered only as collecting and distributing some knowledge about that person, but instead ought to be considered as taking and distributing (parts of) the person herself.

In this chapter I will in section 3.1, as a foundation for the moral unification of the *I* and the *ME*, give an outline of Floridi's (2011) account of the informational person. Based on this account, the person will be conceptualized as a set of information and informational processes, and conceived of as a distributed system, consisting of three kinds of encapsulating membranes, working and functioning together as three agents forming a multi-agent system. In section 3.2, the consciousness membrane's role as a function of unification and coordination of the multi-agent system will be emphasized. Personhood will be suggested as the multi-agent system's or person's degree of informational detachment, that is, as the encapsulation of personal or constitutive semantic information. First, however, I will, in the

[7] This claim will be defended in Chapter 4.

following paragraphs, clarify some central informational concepts that will be useful both in this and the following chapter.

Information objects can, according to Floridi, be understood as data structures and their behaviours bundled together into one package, i.e., into one object of information. An informational object is by this an entity constituted by a set of data[8] (Floridi, 2002, p. 288). The identifying data or property of the object, according to Floridi, "[…] is not determined by its contingent properties as a physical body, including its shape or colour" (2002, p. 288), it is rather its unique data structure, or, in terms of Bates (2006), its unique "patterns of organization", that determines the identity of the entity in question. According to Bates: "The patterns of organization of everything in the universe (other than pure entropy or "patternless-ness") involve every physical, biological, and cognitive pattern of organization that exists or is extracted by sensing beings" (2006, p. 1035). For example, as suggested by Floridi (2002, p. 288) the identity of a pawn in a chess game is not (necessarily) determined by the shape and colour of its physical body. One could be using a cork instead of a pawn by infusing into the cork a pawn's data structure or patterns of organization. For instance, one could decide that the cork is to be one of the eight least valuable white pieces of a game of chess. The least valuable piece having three behavioural rules: "[…] it can move forward, one square at a time (but with the option of two squares on the first move); it can capture other pieces only by a diagonal, forward move; and it can be promoted to any piece, except a king, when it reaches the opposite side of the board" (Floridi, 2002, p. 288). The information object is the sum of the elements, i.e. the set of data that constitutes a whole with its own distinct qualities. In the case of the cork pawn, it is not the physical patterns of organization of the cork that constitutes the "pawn identity", but the distinct qualities of the pawn, that is, in this case, the corks strategic position on the board and its behavioural rules.

The Informational Environment (or in terms of Floridi (1999) *The Inforsphere*) is the

---

[8] According to Floridi the definition of data:

> Dd datum=$_{def.}$ *x* being distinct from *y*, where *x* and *y* are two uninterpreted variables and the relation of 'being distinct', as well as the domain, are left open to further interpretation (Floridi, 2010a, p. 23)

can be applied in three different ways. Firstly data can be understood just as lacks of uniformity (that is, data are differences) in the world, they are then pure data, meaning data (or differences) before interpretation. They are what must be in the world for information (data + meaning and/or function) to be possible. Secondly, data are lacks of uniformity i.e. differences or asymmetries between (the perception of) two, or more, physical states of a system. And, thirdly, data are lacks of uniformity between two symbols of a code, for example the differences between two letters in an alphabet (Floridi, 2010a, pp. 23-24).

environment shared by all *biological and engineered* entities or agents by virtue of their informational character. According to Floridi, the infosphere is a concept that

> [*m]inimally* […] denotes the whole informational environment constituted by all informational entities (thus including information agents as well), their properties, interactions, processes, and mutual relations. It is an environment comparable to, but different from, cyberspace, which is only one of its sub-regions, as it were, since it also includes offline and analogue spaces of information. *Maximally*, it is a concept that, given an informational ontology, can also be used as synonymous with reality, or Being. The difference the two readings is a function of our understanding of information, as something that has only semantic properties (e.g. Wikipedia) or also ontic properties (information as data patterns, e.g. the magnetic structure of a digital support) (Floridi, 2013, p. 6, italics in the original'')

In this thesis a maximal reading of the concept will be adopted.

Level of abstraction (LoA) can be understood as that information of a system that is given attention. According to Floridi, we view any system according to our own interests, which adjust and tailor our choices of conceptual interfaces (or frameworks), i.e. our own levels of abstraction. Any system can be analysed through a range of LoAs, each LoA making possible a determinate analysis or model of the system, with the result that a system can have a range of models (Floridi, 2013, pp. 30-31). LoAs are non-empty finite sets of observables which can be nested, disjoint, or overlapping, and can be hierarchically ordered in some scale of priority. The LoA also indicates the amount of complexity by which a system is viewed, the more LoAs included in the LoA used to analyse a particular system, the more finely grained the analysis of that system. For instance, once a variable *p* is interpreted as for example Mary (*p*=Mary), "depending on the LoA and the corresponding set of observables available at that level *p*=Mary can be analysed as the unique person called Mary, as a Woman, as a human being, as an animal, as a form of life, as a physical body and so forth" (Floridi, 2013, p. 32; 2002, p. 288). In this case, the higher the level of abstraction, the less detail, so the higher level of abstraction the less likelihood for identifying particular individuals. "[I]f Mary is analysed as a human being, more observables could lead one to analyse Mary at a lower LoA as a woman, and less observables could lead one to analyse Mary at a higher LoA as an animal" (Floridi, 2002, p. 288).

By *Encapsulation* I will mean that of separating and enclosing the relevant data structures and behaviour elements from an environment. It is that of containing data and instructions (or information processes) in order to control and reduce improper external manipulation of data and/or information, in order to secure the stability of the system

constituted by this information. Based on this, I will, in relation to informational privacy, define encapsulation as preliminary to and necessary for informational integrity[9]. Encapsulation is to keep the system secure from improper/unauthorized manipulation or alteration of the unique set of information and informational processes constituting the informational system in question in order to promote its sustainability.

3.1 The Person as Information

In this section, as a foundation for a justification of my claim of the moral unification of the *I* and *ME*, and as a preliminary to determining the moral criterion for what information is worthy of protection, I will give an outline of Floridi's (2011) account of the informational nature of selves. This concept will later (in Chapter 4) be suggested as the appropriate re-conceptualization of personhood for an account of informational privacy capable of an adequate justification for informational privacy rights that provides (based on the *direct value* of personal information in relation to the *person* constituted by the information in question) obligatory duties of informational behaviour towards personal information.

One of the pioneers in philosophy of information, Wiener (in Bynum 2008, pp. 8-25) argues that since many animals, particularly humans, can store information within their bodies and use this stored information to adjust future activities, they should be considered as information processors constituted by matter-energy and form (information). Humans as biological organisms need, for their (healthy) continuation, exquisitely organized bodies, with all its parts integrated and working together as a whole by virtue of the parts appropriately communicating with each other. The biological processes within a person's body cause the atoms and molecules that make up his or her body to be exchanged for external ones from the surrounding environment to the effect that all (with the exception of brain cells) of the matter and energy of the body get replaced approximately every eight years. In order, however, to preserve life, functionality, and personal identity, the complex organization or *form* of the body must be maintained by 'homeostatic'[10] biological processes. A person, therefore,

[9] By 'informational integrity' of an informational object I will mean that of preserving the informational object as a unified informational whole (this will be further explained in Chapter 4).

[10] Homeostasis is traditionally understood as physiological mechanisms to protect organisms from damaging variation in physiological factors.

according to Wiener, consists of complex patterns of information embodied in matter and energy, and the human being or person is to be understood as an 'information object' (Wiener, 1954, in Bynum, 2008, pp. 11-12).

In the same vein Floridi considers the self as made of information, that is, "[…] individuation–the characterization or constitution of the self–is achieved through forms of information processing" (Floridi, 2011, p. 555). Information processing is dynamic states of information such as: memory, consciousness, and, personal and social narratives. This presupposes agents endowed with the right kind of informational processes to the construction of personal identities (Floridi, 2011, p. 555).

Floridi argues that the informational nature of a *self* can initially be accounted for in terms of an auto-structuring[11] physical membrane, "[…] which encapsulates and hence *detach* […] parts of the environment into biochemical structures that are then able to evolve into more complex organisms […]" (Floridi, 2011, p. 557-558). According to Floridi, selves are not biochemical, but informational structures, and should be considered as resulting from further encapsulation, detaching the selves further from the external environment. According to the *three membranes model* the person consists of three kinds of information encapsulating membranes: corporeal, cognitive and consciousness. Selves are the results of three phases or stages of the evolution, from physical structures, that is, patterns of physical data of an environment (the world), to the evolution of organisms, then of intelligent animals, and, finally, of self-conscious minds (Floridi, 2011).

In the first phase, physical structures are closed off from their surroundings by a corporeal (or physical) membrane, encapsulating physical data. This allows for a separation of the inside (the structure of the organism, i.e., the individual biotic structure), from the outside (the external environment). The membrane also enables the cell a variety of degrees

---

> Homeostasis depends on control systems which attempt to regulate physiological factors within some bounds. Control systems use negative feedback in which sensors compare the level of a factor against some (possibly variable) set point and produce a signal proportional to the deviation. This signal prompts cells, tissues, or organs to do physiological work to counteract the deviation; the system tries to minimize the error between the measured level of the factor and its set point (Woods and Wilson, 2013, p. 283).

The purpose of homeostasis is by this understood as to provide a stable internal environment for set processes to occur. Each process has a desirable set point. If external influences cause deviation from the set point, the physiological mechanisms will restore stability in a homeostatic organism.

[11] Floridi explain "Auto-structuring" membranes in terms of "auto-assembling and, within the assembled entity, auto-organising" (Floridi, 2011, p. 557) physical membranes. Auto-organizing or self-organizing systems (or, in terms of Floridi, "membranes") are systems with a tendency to spontaneously transform into distinct (and highly complex) patterns (Bawden, 2007, p. 314).

of inputs and outputs with respect to the environment. Data, at this level, according to Floridi, is physical signals broadcasted by other structures in the environment that are captured by permeable membranes of the organism, the body being a barrier between the interior of the organism, and its external environment, protecting the stability of the living system, i.e. the organism's physical homeostasis, and by this enabling the system to use the environment to its own advantage (Floridi, 2011, pp. 558-559).

In the next phase, data becomes encodable resources that can be exploited, through some language or other (it needs not be verbal language but can be sounds, visual patterns, gestures, behaviours etc.), by an organism such as an animal. For example, noises can be made into sounds, and interpreted, through a language, as an alarm. This, however, according to Floridi, requires a cognitive membrane, allowing, by some sort of memory, the encapsulation of data for processing and communication. The stream of data, that in the previous phase was broadcasted quantities without directions, where the source was not targeting any particular receiver, now acquires a direction from sender to receiver, and an interpretation[12]. The body becomes an interface that connects the system with its environment, enabling communication with the world. According to Floridi, the cognitive membrane is a configurable or semi-hardwired divide or barrier that detaches the cognitive system from its environment or surroundings. This further detachment allows the organism to exploit data processing and communication. In this phase, according to Floridi, the stability that is to be sustained by means of the cognitive membrane is a stable environment for the internal data within the system together with the membranes information processing powers, that is, its memory and language (i.e. the system's codification) (Floridi, 2011, p. 559).

---

[12] According to Floridi (2011, p. 559), from this phase or stage on, Shannon's communication model sets in. According to Shannon's communication model, a selected message flows from an information source, i.e. a sender through a transmitter that converts the message into a signal, that is, through an encoder. The communication channel then conveys the signal to a receiver where a decoder converts the signal back into a message; the receiver interprets the message, and sends the message to its destination (which may be another receiver or the message may rest with the initial receiver) and communication is achieved. In Shannon's mathematical theory of communication, information is treated as data communication, that is, as the transmission of information that has been encoded or converted for storage and processing (Floridi, 2010a, pp. 37-42). For instance (here exemplified by a simplified description of the workings of human hearing), in the above case of noise made into sound interpreted as an alarm; a noise (i.e. "[…] mechanical disturbance of the medium, which may be air, or a solid, liquid or other gas" (Howard and Angus, 1996, p. 1)) is captured by the tympanic membrane which converts it into mechanical vibrations to the inner ear. These mechanical vibrations are then, by the function of the cochlea of the inner ear, converted into nerve impulses (Howard and Angus, 1996, pp. 67, 71). By this, the cochlea is a transmitter that encodes or converts the incoming signals into a suitable form for transmission and conveys the signals to the cognitive membrane. The cognitive membrane (by its information processing powers i.e. its capacity to store information and its capacity for language) converts the received signal back into a message, i.e. a sound, and interprets it as an alarm.

Floridi describes the third phase as the evolution of the consciousness membrane where data become *repurposable* information. That is, with the evolvement of the consciousness membrane, environmental information[13] can be reused or repurposed by the cognitive strategy "[…] of using, converting or modifying data/signals for a purpose or function […]" (Floridi, 2014, p. 88), such as when sounds become a national anthem (Florid, 2011, p. 559). This is similar to Grice's notion of nonnatural meaning (or information). Under this notion, the sentence "Those three rings on the bell (of the bus) means that the bus is full" carries its meaning or information by virtue of convention (Grice, 2010, p. 108). The membrane is thus programmable or soft-wired and the body becomes the outside surroundings for an inside experience, the stability or mental homeostasis that is to be maintained within the consciousness membrane is that of the self within the system. According to Floridi, the evolvement from the previous phase consists in the move from aware to self-aware, systems (Floridi, 2011, p. 559).

On Floridi's account of the informational person, each membrane can be understood as different degrees of informational detachment or separation from the world, where each membrane can be considered an *autonomous* system or agent[14]. As a result, the corporeal membrane, the cognitive membrane, and the conscious membrane, can, from an informational perspective, be understood as parts of a unitary system, with the three membranes or agents forming a multi agent system.

On the level of the corporeal or biological membrane, information is "[…] information *whose* nature is biological (genetic) in itself" (Floridi, 2010a, p. 75, italics in the original). For instance, the data structures encapsulated in the corporeal membrane include DNA structures where DNA molecules are organized into structures to the effect of the

---

[13] In this context *environmental* information can be assimilated to Grice's notion of natural meaning (2010). According to Floridi, environmental information is information that can be meaningful independently of an intelligent producer or informer. Environmental information consists in physical correlations, such as the correlation between the concentric rings emerging on the wood of a cut tree trunk and the tree's age. Each ring is an effect of the tree's growth of one year. Although this information can be used to estimate the tree's age, but the rings (i.e. "the pattern of organization") *means* the tree's age irrespective of evaluation (Floridi, 2010a, pp. 32-33). For instance, in terms of Grice (2010, p. 108): "Those spots means measles", is true whenever there is a physical correlation between the spots in question and a morbillivirus regardless of any agent recognizing their correlation. By this, environmental information does not require semantic content since environmental information consists of correlated patterns or data structures understood merely as physical differences or asymmetries Floridi, 2010a, pp. 32-33).

[14] 'Autonomous' meaning that the agent or system encapsulate some state that is not accessible to other agents, and based on this state "make decisions" on what to do; the system is situated in an environment and is able to respond to changes that occur in it in a timely fashion. It can cooperate and be coordinated with other agents to the effect of forming a multi-agent system (Ciancarini and Wooldridge, 2002, pp. 2-3).

storing of the organism's genetic code. The genetic code or the genes stored or contained in the DNA are the information itself, and they are performative instructions in that they do not describe but perform more or less successfully depending on environmental influences (Floridi, 2010a, pp. 76-79). The interaction between the system, i.e. the agent (the corporeal membrane) and the environment (the world) takes place through the corporeal agent's permeable structure[15]. As mentioned above, in the first evolutionary phase, a corporeal detachment or decoupling of the living system (or organism) from the environment (or the world) is taking place by corporeal elements fitting together in the structure of a body bound together by chemical bonds and orientations (Floridi, 2011, p. 560).

At the next stage, however, instead of a physical encapsulation or detachment from the world, a cognitive detachment or encapsulation is occurring by the emergence of perception. According to Floridi, perception or perceptual experience is the process through which information about the world can be acquired. Data as signals are elicited by sensorimotor interactions between an agent and an environment. At this second stage the data perceived do not generate propositional semantic information, the perceived signals (data) have, however, according to Floridi, semantic value or meaning to the extent that the signals put the receiving agent in some state. That is, the signals are interpreted and made meaningful by putting the perceiver in a certain state (Floridi, 2014, pp. 77, 83-84). According to this I understand the data processing taking place in the cognitive membrane as relating to the perceiving and interpretation of signals (data) (such as perceiving noise and interpreting it as sounds putting the perceiver into a state of alarm) to the effect of providing information for appropriate action. I understand the cognitive homeostasis (or stability) to concern the process' guiding capacity, that is, the capacity the semi-hardwired agent (i.e. cognitive membrane) has to providing accurate information for appropriate action. The semi-hardwired agent needs at this stage no capacity for understanding and explaining the information in question. At this stage the semi-hardwired agent, or the cognitive membrane, provides a further detachment from being fully absorbed by the world by bonds and orientations provided by mutual information, that is, by the measure of the interdependence of data. When smoke and fire are two random variables, the mutual information of smoke and fire is a quantity that measures the mutual dependence between them. At this stage corporeal and

[15] The same data can, however, be understood as "information *about* biological (genetic) facts" (Floridi, 2010a, p. 75, original italics). But for information to be understood in this way, a cognitive and/or consciousness membrane is required.

cognitive elements fit together in structures of body and cognition (Floridi, 2011, p. 560).

In the final phase, propositional semantic information is generated by the process of testimony of data, i.e. the "inside" experiences, encapsulated by the consciousness membrane. According to Floridi, in the final phase the body becomes an outside environment for an inside experience. Data as signals are elicited by the interaction between the agent (now the soft-wired or programmable consciousness membrane) and the body (the hardwired interface), and they are *repurposed* for epistemic, communicative and semantic goals (Floridi, 2011, p. 559; Floridi, 2014, p. 88). By repurposing data what is meant is

> [t]he cognitive strategy of using, converting or modifying data/signals for a purpose or function other that their original natural one, to fit a new use [such as when] a cloth becomes a flag, which becomes a country, which becomes a foe to burn, or something to be proud of and wear as qualifying one's identity, and so forth (Floridi, 2014, p. 88, my insertion).

The repurposed perceptual data are used as resources to interact with the world by constructing semantic artefacts to the effect of a detachment from the world that goes even further than the detachment occurring at the previous stage where information was limited to perceptual experiences of quantitatively measured mutual dependencies between data. At this final stage the corporeal, cognitive and consciousness elements fit together in structures of body, cognition and mind (Floridi, 2011, p. 560)[16].

A person can accordingly be understood as a set of all three membranes. This means that the genetic information which is encapsulated by the corporeal membrane just as the semantic information encapsulated by the cognitive and the consciousness membranes is part of the whole set of information that makes up an individual or person. Based on Floridi's account, I take it that an individual entity consists of a unique set of information according to the individual's level or degree of encapsulating membranes. Each membrane is a subset of

---

[16] Floridi's view is here similar to Bawden (2007) who argue that: "[…] the origin of life itself may best be viewed as an informational event, as is the subsequent evolution of all life, and the development of intelligence and culture […]" (Bawden, 2007, p. 315). Information in the Physical domain can be seen as patterns of *"organised complexity* of matter and energy", in the biological domain information can be viewed as "*meaning in context"* emerged from the self-organized complexity of matter and energy of a biological organism, information in the human domain can be viewed as understanding emerging from complex interactions with the internal mental states of a conscious individual, and the mental product of the human consciousness emerging from interactions with the world of communicable information, where the unifying concept of information in the evolution, is organised complexity (Bawden, 2007, p. 318). An informational event is a change in organised complexity, and where life is an example of self-organised complexity *"par excellence"* (Bawden, 2007, p. 315).

decoded data according to its particular level or degree of encapsulation. A person can, accordingly, be conceptualized as a distributed system[17]. The three membranes, or agents, form a loosely combined network, working and acting together and appearing as a unity, sharing information processing powers at specific levels of encapsulation, using its own information to adapt or adjust itself, in order to maintain stability of the system[18].

3.2 Self-Individuation by Semantic Information and Personhood as Informational Detachment

The above argument suggests that a person *is* nothing but a set of information and information processing powers. In terms of Hongladarom: "[…] anything one encounters when one encounters one's own self is nothing but information" (2011, p. 362). In this section I will give a brief account of the individual as a unique set of information, and argue that this information is not to be considered as knowledge about a person, but as constitutive parts of the person itself. Personhood will be suggested as the "right" degree of informational detachment, that is, as encapsulation of personal or constitutive semantic information. I thus suggest that informational privacy rights, as protection of personhood, should be conceived of as the protection of the multi-agent system's informational detachment due to its degree or level of informational encapsulation.

By adopting Floridi's account above[19], it becomes clear that, to the effect of individuation, by accumulating semantic information of data from its agents, the consciousness membrane generates testimonies or statements of the system and creates a unity of the system as a whole by organizing them into a unique narrative or interpretation of itself. I think this is well explained by Hongladarom:

> […] Now suppose that we can accumulate all the statements about one's body throughout a period of time, as well as statements describing one's mental episodes as they progress through his or her life. It does not seem too farfetched to conclude that

[17] According to Zang, et al., (2004), a distributed system is a multi-agent system consisting of (semi) autonomous agents forming a "loosely coupled network", working together to solve problems that are beyond the capability of its individual agents.

[18] This will be further discussed in Chapter 4 in relation to claiming the direct value of personal information.

[19] One's "physical life" is constituted by biological information, encapsulated in the corporeal membrane, and one's "mental life" is constituted by series of perceptual events or experiences encapsulated by the cognitive and consciousness membranes (Floridi, 2011).

> these statements taken together represent the account of that person's self. After all, the self is given content through these statements which are true of it and which all together give it its uniqueness vis-à-vis other selves. For example, I have my own unique narrative which constitutes my life story. Everybody has his or her own unique story that accounts for his or her own self. But if it is story, if it is narrative, that gives a self its uniqueness, its standing as a self, then it seems that the self is constituted through information, for it is information that is contained in the statements that make up the narrative of a self (Hongladarom 2011, pp. 362-363).

In Floridi's line of thought, what makes humans uniquely different from (and more successful than) other species (from an evolutionary perspective) is the level of detachment of the information from the world by the consciousness membrane's "[…] semantic incapacity of being absolutely and inseparably present, cognitively, where we are located, bodily" (Floridi, 2014, p. 92). I take the degree of encapsulation of the information in the consciousness membrane to create a distance of the multi-agent system to itself to the effect of its unification. That is, by the degree of encapsulation of information by the consciousness membrane, the multi-agent system i.e. person satisfies the condition of distance required for observation. Due to this distance, that is, due to the degree of informational detachment of the consciousness membrane, the multi agent system is enabled to be its own object of observation. As mentioned in section 3.1, information encapsulated in the consciousness membrane is that of semantic information. Semantic information, however, according to Floridi, requires a capacity to "[…] interpret something as something else" (Floridi, 2010b, p. 276). At the level of consciousness this is the capacity to make testimony of data. Accordingly, due to the information and information processing powers of the consciousness membrane, the system can observe, make interpretations and testimonies of its own data structures to the effect of the multi-agent system's capacity to unify its information in form of a unique coherent or cohesive narrative (or what I in Chapter 4 will refer to as the multi-agent system's self-model). In other words, the consciousness membrane serves as a function of unification or coordination of the multi-agent system by generating a detachment or distance necessary for self-observation, and by that providing for information processing powers capable of constructing a unique coherent self-narrative (or model) to the effect of coordinating its agents.

By this, the resulting collection of testimonies or statements, which express the *uniqueness* of the system in question, is the set of information which constitutes the individual multi-agent system. That is, the uniqueness of the set of information is what distinguishes one individual multi-agent system from another. Each individual person is by

this a unique set of three sub-sets of information, encapsulated by the three constituent membranes or agents of the multi-agent system together with the kinds of processing powers appropriate for the agents' respective levels of encapsulation. According to Floridi, a person can be described as

> […] a discrete, self-contained, encapsulated package containing the appropriate data structures, which constitute the nature of the entity in question, that is, the state of the object, its unique identity, and its attributes; and a collection of operations, functions, or procedures, which are activated by various interactions or stimuli (that is messages received from other objects or changes within itself), and correspondingly define how the object behaves or reacts to them (Floridi, 2010a, p. 111).

By this, information activates the system or person's processing powers to the effect of information being what converts the system into a reactive form, the system being an interdependency of information and information processing powers. The person or multi-agent system can thus be said to be a unity of information and processing powers, or, in other words, a unity of *I* and *ME*[20]. By information being what converts the system into a reactive form, information is constitutive of the system in question. Accordingly, when making information from such a set accessible or available to others, one is not sharing knowledge about a unique collection i.e. person with others, but distributing parts of the set/collection i.e. the person itself.

In relation to informational privacy, since the person is not necessarily to be considered an entity separated from its information, but as an entity consisting of and constituted by information, a theory that separates personal information from the person in question, and considers personal information (only) as a product or commodity of the agent, is mistaken. There is no agent apart from the information and information processes encapsulated and detached from the world by the structural membranes of the system. That is, in informational terms, in the final phase of evolution, even the self-conscious mind is information. Thus, when information from my unique set (the *ME* set) is taken from this set without my consent, *ME* or at least parts of *ME* can be conceived of as being taken at the risk of injecting instability into the system in question. For instance, in the originate set the capacity of storage is limited. When information is taken from this set without authorization and stored elsewhere where the capacity of storage may be unlimited or at least greater than in the originate set, the unauthorized copied set (i.e. the sum of all sub sets of unauthorized

[20] Recall that in section 2.2 the *I* was conceived of as the active part of the self.

copied information) could be larger than the original set. In other words, a copy of ME could be larger me than *MYself*. On the other hand, the unauthorized, copied information can then be distributed back to the original set. When information is what the person is made of, and this information is distributed back to the originate set, the originate set is added to by information not authorized as part of the set by the originator (the originate set). The originate set is by this *manipulated* by agents external and unknown to the set in question, and a new extended set is constructed. Even if the information cannot be said to be removed from the set it is taken from, but only copied, this does not mean that when information from a unique set or collection of information is accessed by someone, the person (set) who consists of the accessed information, is not at the same time being approached *herself* by the one accessing the information in question. By accessing and copying personal information, that is, information from an original unique set (of the appropriate degree of detachment) without authorization, the informational self is sustained at the mercy of others, since the originate set can easily be altered by copied information being distributed back to it. By virtue of new ICTs that can be designed to accommodate more or less unrestricted access and distribution, the person is susceptible to unrestricted manipulation[21].

As a system of informational agents, a person shares an *informational environment* or an *informational world* (or the *infosphere*, in terms of Floridi (1999)) with all other informational entities. Recall that the informational environment is an environment shared by all biological and engineered entities by virtue of their informational character.

Our interaction is to a greater and greater extent taking place within this informational environment or world. Since, from an informational perspective the person can be conceptualized as a collection of information, it would not seem implausible that through the development of new Information and Communication Technologies (ICT), we would be able to, by eliminating "natural" encapsulation of information open up for unlimited distributions of persons that could jeopardize the identity of multi-agent systems. For instance *ubiquitous computing*[22], a fairly new and rapidly evolving type of computing technology, can diminish corporeal encapsulation of information by constructing or designing applications by which a

---

[21] This will be further discussed in the following chapter.

[22] Ubiquitous computing means "computer processing power everywhere", in every technological artefact constructed, to the effect of these artefacts being able to communicate with each other by being integrated into a computer network. Computing power is no longer residing only in "normal" computers but also in everyday familiar devices not normally considered as computers, such as, a refrigerator to the effect of the refrigerator, for example, being able to communicate with the grocery store (Hongladarom, 2011, pp. 360-361).

human body and an external unit or device can be integrated into a computer network in order to be able to communicate with each other. For instance "[…] when certain physical indicators fall below a certain threshold, data can be sent out from the sensor in or on the body to the medical unit in order for the latter to take appropriate action" (Hongladarom, 2011, p. 361). Such an enmeshment of the body in a network is already a reality[23], it is thus not implausible, from an informational perspective at least, that also data or information encapsulated in the cognitive and consciousness membranes can become integrated into the network. One can thus, according to Hongladarom, imagine that by means of ubiquitous computing bodies and minds can be spread out (that is distributed) throughout a network[24], and with the occurrence of such a distribution, that is, "[w]hen bodies and selves are spread throughout the network, their interaction will not be merely the case of two skin-encased bodies talking with or touching each other, but in a sense, it will be the case of two network bodies fusing and emerging with each other" (Hongladarom, 2013, p. 232). Although some might reject such a scenario as unrealistic[25], it emphasizes (in my opinion at least) the function of encapsulation of the consciousness membrane. By having direct access to information in external consciousness membranes, that is, by having direct access to others' feelings and thoughts (as though they were one's own) we would be risking our ability to self-differentiate to the effect of endangering the stability of the system. By having direct access to, for example, others hunger beliefs as though they were "mine", it might result in "me" overeating, and by the other having access to my belief that I have eaten and is full, as though it was her own information, this person could be risking starvation. This kind of external manipulations of information would, in both multi-agent systems, cause unstable or chaotic patterns of food consumption.

---

[23] Recall the example of life-logging in section 2.2.

[24] Hongladarom argue that, assuming one could, "by installing a device in the brain that senses the electrical movements inside the brain representing various thoughts and desires and sending out information of these movements to a network" (Hongladarom, 2011, p. 362) it would be possible, even without the person's conscious awareness, for a person's mental episodes to be sent out and accessed *directly* by others (Hongladarom, 2011, p. 363). Hongladarom seems to think this as a way of enhancing the world. According to Hongladarom, by having *direct* access to other's thoughts and feelings - as opposed to a world where empathy seems secondary by having to infer the content of others' thoughts - one could have full empathy towards others and this would, according to Hongladarom, contribute towards a less cruel and evil world (Hongladarom, 2013, p 234). In my view, this shows another side of privacy. Our need for limiting access goes both ways. Privacy does not only protect us from others' excessive access to ourselves, but also protects us from having an overwhelming (i.e. direct) access to others' thoughts and feelings. I will, however, not elaborate on this here.

[25] Bates, however, claims that as information scientist one accepts that the subjective constructions a person creates of her experiences, that is, the information encapsulated in the consciousness membrane, have an objective existence in the nervous system or the brain of the person in question (Bates, 2006, p. 1035). By this, Hongladarom's proposed scenario (described in footnote 24 above) does not seem implausible.

Through new informational technologies, giving rise to increasingly more pervasive distribution networks, we are increasingly subjected to extensive (both authorized and unauthorized) distribution of ourselves throughout the informational environment, that is, we are increasingly subjected to extensive connectedness through distribution. Personhood, on the other hand, emerges from the consciousness membrane's degree of informational *detachment* from its environment, and we are dependent on freedom from being subjected to improper or unauthorized external manipulation of our own personal informational in order to remain a stable and complete unity. An unauthorized copied (sub) set of information can endanger the stability of the original set by subjecting it to a destructive connection with its informational environment.

Even without the grim prospects of a fusion as described above, I believe the informational account of personhood and individuation (i.e. the person as a detached collection of information) can provide more sufficient or adequate grounds for a justification of informational privacy rights than the above mentioned liberal accounts. If the encapsulating membranes, due to the development of more pervasive ICTs, no longer can provide a sufficiently robust shield for the information it is encapsulating, but leaves this information vulnerable to interference or manipulation by external agents within a network, the stability of the system could be at risk. Thus, on the account of the informational person, violations of informational privacy it is not *only,* as claimed by Benn (1988) and Rössler (2005), threatening a person's autonomy, but the informational person herself. Since information encapsulated within the three membranes is constitutive of the person, if persons have a (moral) claim on others' respect, such a claim should include respect for the information that is constitutive of them.

My aim here is not to contest the value of autonomy in general, only that the value of autonomy (because informational privacy concern person constitutive information) does not give a sufficient foundation for informational privacy rights, since these theories do not recognize the moral status of such information. Informational privacy should rather be considered from an informational perspective, from which the value of personal information can be appropriately defined, and the moral status of personal information can be recognized.

The rest of the thesis will be dedicated to defending my claim.

In the next chapter I will outline the weaknesses of the moral criterion implicit in the liberal theories and through this develop a moral criterion for informational privacy of informational

agents based on the conception of *encapsulation* i.e. self-organization or unification as the foundation for the right to informational privacy.

4 The Moral Criterion for Informational Privacy: The Direct Value of Personal Information

In the previous chapter I argued for the conception of informational personhood, as opposed to a conventional liberal conception of autonomy, as the appropriate concept of personhood for providing a sufficient justification for informational privacy rights. My claim was that informational privacy rights should not be grounded on autonomy alone but rather on a concept of "the person as information".

In this chapter, I will attempt to justify this claim by arguing that the crux of informational privacy is not autonomy in self-presentation but rather that of preservation of informational selves i.e. the preservation of multi-agent systems of the right degree or level of encapsulation or detachment. The right degree of encapsulation or detachment being that of the multi-agent system's privileged position, of the first-person LoA[i], to organize its constitutive information coherently, in order to make itself into a unified model, to the effect of optimizing itself as *perpetuating* or *homeostatic* information patterns[26]. I will then develop a moral criterion for informational privacy based on the informational conception of personhood. My aim will be to show that the re-conceptualization of personhood from autonomy to personhood as the degree of informational detachment in a consciousness membrane should result in rearticulating informational privacy rights as rights to informational integrity rather than rights to control access to one's personal information.

By informational integrity I will mean that of preserving the wholeness or unity of the informational person, or in other words, preserving the informational set (person) at the right level of detachment or separation from the world, by preventing corruption or improper alteration or manipulation by external informational agents, and by that sustaining or promoting the internal coherence of the informational person (set).

Based on this, I will suggest the right to informational privacy as the right to freedom from *improper* external manipulation of personal information. This reformulation of informational privacy right as the right to informational integrity will provide precise normative criteria for what information is to be protected by informational privacy right. I

---

[26] I have borrowed these terms from Wiener (1954, in Bynum, 2008, p. 18) and Floridi (2013, p. 310) respectively.

will claim that by understanding informational privacy rights as rights to informational integrity, the right to informational privacy will emerge as a fundamental right not easily overridden by opposing interests, while simultaneously being flexible enough to cater for some necessary exceptions. In order to account for this view, an informational LoA will be adopted as the appropriate normative framework for informational privacy and a distinction between *direct* and *indirect* value will be claimed, the former being attributed personal information.

The concern of any theory of informational privacy is to account for the value of personal information, any theory, which can adequately account for the value of personal information, will also provide for a sufficient justification of informational privacy rights. According to Benn (1988) and Rössler (2005), personal information is only valuable in relation to the value of autonomy in that informational privacy sustains the agent's status as an autonomous agent and this status is held as a fundamental value. By such views, personal information has only an indirect value, that is, its (potential) value is justified and measured by another (fundamental) value, i.e. autonomy. From an informational LoA, on the other hand, personal information is constitutive of the person, that is, a person is an information object. Constitutive information is the elements of a *core* or *nucleus* set of information of the multi-agent system. By this I mean that information that cannot be constitutive, i.e. a member or element of another set. In other words, personal information is that information, either as a single piece, or in a combination, which is unique to a particular (informational) person. Since manipulations of the *core* or *nucleus* set of information can cause corruption of the person as an information object, keeping this set of information from improper manipulation is necessary for sustaining the information object in question.

A distinction can thus be made between what I will refer to as *direct* and *indirect* value of personal information. By personal information and thus informational privacy having a *direct* moral value I mean a *relational* notion of value, similarly to the one defended by Moore (2010), where value is attached to an object or state that "[…] sustains, promotes, or furthers […] the entity in question" (Moore, 2010, p. 38). I suggest *direct* value, as the value personal information has by virtue of its (internal) relations, that is, its membership in the *core* or *nucleus* set of information, which constitutes the entity in question. *Direct* value is opposed to *indirect* value or potential/conditional value, or, in other words, value on the condition of some other value or good. This means that when the entity in question is the informational person, its personal information, i.e. its core or nucleus set of information, is

valuable in itself in relation to constituting or being that person, and not potentially valuable on the condition of some other good. Since, on an informational normative framework, no moral distinction is to be made between the person and her information, I will claim that this distinction will lead to the justification of personal information being ascribed moral status.

Himma (2004) argues against Floridi's (2002) claim that that information is intrinsically valuable and is thus deserving of at least some minimal moral respect. I am not considering this debate here, I will however make use of Himma's argument of intrinsic value in order to convey my view on how moral value can be ascribed to personal information due its direct value in relation to the multi-agent system. According to Himma, "intrinsic value" can, on the one hand, be understood as that which characteristically is valued for its own sake by an evaluator. What people characteristically value for its own sake is then either considered as the sole ground of moral worth, or at least, that people have some morally protected interest in that which they characteristically value for its own sake (Himma, 2004, p. 146). On the other hand, "intrinsic value" can be understood as, to borrow a term from Korsgaard (1996, p. 250), "it has its goodness in itself", value here referring to the source of the goodness (Korsgaard, 1996, p. 250). That is, when talking of "intrinsic value" in this sense, one is looking for identifying the source as a class of objects or entities that induce obligatory constraints on others' treatment of it. In other words, it is this kind of value which gives rise to moral standing or status. An agent or person has moral status, that is, is to be considered a moral entity because others may not treat her as a mere means. A moral entity thus has a claim on others' respect (Himma, 2004, p. 146). According to Himma, (personal) information cannot be considered as having moral status because

> [t]o say that we value information for its own sake is to say that it is intrinsically good for beings like us that have moral standing. But while this claim may imply that it is morally good, other things being equal, that beings like us have information, it doesn't imply that information has moral standing in the sense of being owed obligations. Happiness is valued by us for its own sake, but this simply means that it is morally good for moral patients who intrinsically value happiness; it does not imply the very counterintuitive claim that moral agents owe an obligation of respect *to* happiness (Himma, 2004, pp. 155-156, italics in original).

Even though knowledge is not uncommonly pursued for its own sake, it is only in relation to knowledge seeking agents that information by virtue of being knowledge can be valued for its own sake (Himma, 2004, p. 155). Accordingly, information can only be considered as having intrinsic value in the former sense in terms of the intrinsic value of knowledge in

relation to an agent with moral status, and thus, (personal) information cannot be ascribed moral status.

My claim is that Himma (2004) is mistaken in that moral value ascribed information necessarily leaves information void of moral status. I will suggest my notion of the *direct* value of personal information as an alternative, in which the moral status of (personal) information is provided for by its relation to the set of which it is a member.

As mentioned above, according to Himma (2004), there are two different ways in which to understand information as having "intrinsic value", one is to consider information or knowledge as characteristically valued, by moral entities, for its own sake, the other is to consider the value of information as an entity itself worthy of respect i.e. as a moral entity. While differentiating between two senses of "intrinsic value" only one of which generates moral status, Himma (2004) (in the vein of Floridi (2002)) does not distinguish between two types of information: information with direct moral relevance (moral-relevant) in relation to the entity in question, and information only indirectly morally relevant (in this context, moral-irrelevant), in the sense of Himma's account of the first kind of intrinsic value. Moral-relevant information i.e. person-constitutive information is, by virtue of its direct value of its person-constituting properties, generating moral status because there is no distinction between the person having moral status and her information.

Himma (2004, pp. 155-156) compares the value of information to that of happiness, however, in case of happiness, a clear distinction can be made between a state of happiness and the person being happy (that is, I am not happiness, nor is being happy necessary for my existence), in the case of personal information, on the other hand, no clear distinction can be made between a unique set of information and the informational agent being that information (recall in Chapter 3 the informational person was conceptualized as packages or sets of information and information processes activated by this information). According to Himma, (personal) information is valuable only in relation to a moral agent separate from its information, and so, no moral status is ascribed to the moral-relevant information of the agent. On the other hand, when no distinction is made between the moral agent and her moral-relevant information, i.e. the information constituting the person, it becomes evident that it is not appropriate to compare the value of this information with the value of happiness. The state of being happy might be a valued state for a person to be in, but happiness is not a necessary property of the person, that is, it is not a constitutive part of the person. On the other hand, by virtue of being an element of the entity's core or nucleus set of information,

the *direct* value of personal information for the informational entity is that of both constituting and sustaining the entity in question.

The value of personal information is relevant to a multi-agent system, due to the particular relation it has to its own personal information, as a distributed system. Since this system is consisting of three membranes (i.e. a corporeal, cognitive, and, consciousness membrane) forming a loosely combined network, acting together *appearing* as a unity, and sharing the processing powers of collecting and manipulating data or information in order to create and maintain stability for the whole system. The multi-agent system thus "[…] uses its own information to modify itself […] to enhance its survival, responding to both [external] and internal stimuli to modify its basic functions to increase its viability" (Collier, 2004, p. 164, my insertion). The relation it has to its own personal information is that of constructing out of this information a coherent or unity of information consistent with the data this information is extracted from.

The state of informational privacy[27] is what protects the self-constructed unity of personal information from being (improperly) manipulated. Informational privacy, thus, directly preserves and furthers the informational integrity of the person, i.e. the person as an informational object. As will become evident below, the importance of adopting an informational normative framework when considering informational privacy rights, is that by such an adoption informational privacy is not dependent on a separate and more fundamental value in order to be justified as a fundamental right, neither is any additional social or conventional framework required to specify its applications.

In the following I will first (in section 4.1) consider the consequences of not recognizing the direct value of personal information, I will claim that a theory of informational privacy not recognizing the direct value of personal information cannot provide the forceful and complete rights to informational privacy needed for adequate protection within the digital informational environment. In section 4.2, I suggest that a distinction between the *natural* and *informational* person should be understood as a distinction in LoAs and not as an ontological distinction. I will argue that when the "natural" person is identified with the "informational" person, the direct value of personal information will become apparent, and the moral status of personal information can be recognized. In section 4.3, I

[27] The state of informational privacy will, in section 4.4 of this chapter, be suggested as the "informational" state of having one's *core* or *nucleus* information successfully encapsulated or encased within the appropriate membrane(s), and by that, protected from improper or unauthorized external manipulation.

will formulate an account of how the content of personal information is to be determined. Then, in section 4.4, I will define the harm in taking this information as the harm of informational fragmentation, or informational de-unification, of the multi-agent system or informational person, with the accompanying risk of de-stabilizing the system or person in question. In section 4.5, some objections to the informational re-conceptualization of personhood and informational privacy rights based on this re-conceptualization will be anticipated and briefly discussed.

As mentioned in Chapter 1, this thesis is concerned with finding a moral foundation for informational privacy rights. The objective of this chapter is to find a precise criterion for what information is worthy of protection and to explain the moral concerns in taking this information. I will claim that by recognizing the direct value of personal information, informational agents will be placed under obligatory constraints with regards to their informational behaviour. Due, however, to the limited scope of this thesis, the content of such moral constraints and the conditions for justificatory exceptions, cannot be developed further here. Although, as an initial step, I think moral constraints on informational behaviour must be considered as constraints relating at least, to both collection and distribution, such as, if/when collection can be justified, obligatory constraints on distribution will still stay in place. This task, however, must be left to future work.

4.1 The Value of Informational Privacy Rights as Indirect

The value of personal information has, conventionally, been stated as conditional upon some other value taken as fundamentally valuable. Rössler (2005), for instance, argues that personal information is worthy of protection only on condition of the fundamental value of autonomy. I will, in this section, consider the implications of taking a roundabout way in accounting for informational privacy rights, and point to some obvious inadequacies in theories taking this stance, particularly in view of the revolutionary developments of the informational environment.

According to Benn "[a] person enjoys privacy as of right if he possesses the normative capacity to decide whether to maintain or relax the state of being private" (1988, p. 266). On the other hand, a person has an interest in privacy if he would be better off (in their

own view) either if he was in a private state or had the power to control access to it (Benn, 1988, p. 266). In Benn's view we have a special interest in privacy (as access control) because free access by others to information about ourselves will make us "vulnerable to discrimination, victimization, or blackmail" and by that threaten a person's freedom (1988, p. 293). According to Rössler, the reason why informational privacy matters so much to people, is the value they place on having control over their self-presentation. Informational privacy provides them with control over "how they want to present or stage themselves, to whom they want to do so and in which contexts […] over how they want to see themselves and how they want to be seen" (Rössler, 2005, p. 116). Violations of informational privacy entail a loss of such control and "[…] implies a disruption of the […] well-founded, *normative* […] horizons of expectations that a person has regarding the knowledge that others may justifiably or legitimately have about her […]" (Rössler, 2005, p. 114). The legitimacy of ones expectations rests, according to Rössler

> […] on the validity of social conventions and norms, which regulate […] what counts as worthy of protecting and as intimate, what is viewed as a legitimate shield or zone protecting a person from public attention or control, in other words what is to be subject to individual information control and what is not. These expectations are regulated, therefore, by a complex, but nonetheless stable fabric of social norms and conventions within which we operate and control the various relations in which we live (Rössler, 2005, p. 118).

These norms, establishing what is to be considered public on the one hand, and what is to be considered private on the other, can be understood as articulations of a normative principle, guaranteeing both negative liberties and the positive possibilities for living these out. This means, according to Rössler, that the conventions regulating informational privacy must in the end be "validated in terms of this principle guaranteeing individual autonomy" (2005, p. 118). The moral criterion for what can legitimately be accessed without authorization by the person in question is, according to Rössler, established through social norms and conventions grounded in established civil liberties. Unauthorized access to a person's information that does not jeopardize any civil liberties entitled to her is *not* regarded as violations on this person's informational privacy. What distinguishes illegitimate from legitimate collection of personal information is the (actual or possible) effect such collection has (or can have) on the person's autonomy. Rössler's claim is that the reason for valuing privacy is that of placing value on autonomy, "personal" information as such is thus not to be ascribed any moral value. On these grounds, Rössler recognizes four groups of data in order to determine what

data are to count as worthy of protection[28]. These data are as such, according to Rössler, neither personal nor valuable, but their informational significance, that is, "[…] when these data become 'personal' in nature or when legitimate data collection ceases to be so, as well as when data can be used to identify a person […]" (2005, p. 124), is relative to the context in which they occur (Rössler, 2005, pp. 124-126).

Rössler does not recognize personal information as a particular kind of information in justifying informational privacy rights. In Rössler's view it is not the particular information that has been accessed without authorization that determines privacy violations. It is rather the contexts, in which this information is accessed, that that can turn unwanted or unauthorized access into privacy violations (Rössler, 2005, pp. 124-125). Benn argues that that one is entitled to access and collect others' personal information if this information is relevant to a legitimate purpose (and not particularly sensitive). A prospective employer is, for example, entitled to ask former employers about the applicants' competence. On the other hand, the employer is not entitled to information not relevant to the job, such as perhaps race, religion etc. since this kind of information will give the employer the ability to discriminate in the recruiting process, on irrelevant grounds (Benn, 1988, p. 293). Similarly, Rössler claims that what information can justifiably be accessed, collected, and distributed by others without the consent of the person in question, depends on the interested parties, who they are and their motivation or reason for accessing, collecting, and distributing the 'personal' information in question. Legitimate motives for collecting personal information are motives or reasons that are in themselves not intentions of control. Motives of efficiency or profit, for example, can be legitimate motives for collecting and distributing personal information since these incentives as such are not intended as constraining the person's civil liberties, guaranteed by a liberal democracy, and as such do not violate the person's informational privacy. On the other hand, if or when these incentives or motives turn into a matter of control, without the knowledge of or against the will of the person being controlled, they should be considered harmful to the person's civil liberties, and thus illegitimate (Rössler, 2005, pp. 123-125). It is puzzling, however, in my opinion, when Rössler defines violations of informational privacy as the constraining effect information gathering has on a person's autonomy in self-presentation on the one hand, but justifies legitimate contexts of collecting

[28] These groups include thoughts and mental states, feelings and views in general; personal data that can provide information of the person's preferences, traits and habits; data about (legitimate) activity in one's own home; and data about activities performed in public and "spatiotemporal facts about a person" (Rössler, 2005, pp. 122-124).

information by turning to motives for collecting on the other. To me it is not clear that these correspond, that is, it is not clear why the motives of the collector, and not the collecting, is what affects the way I choose to present myself. As Rössler points out,

> [w]hat persons are willing to recount or divulge about themselves in various contexts differs greatly according to the individual concerned, as well, of course, as the culture. The fact that there are these individual differences clearly has nothing in itself to do with the degree of autonomy in the person. There is obviously a degree of leeway as to whether people are more or less open or reserved, or show a greater or lesser need to communicate with people […] (Rössler, 2005, p. 118, footnote 20).

However, if the value I place on my autonomy in self-presentation is what justifies my right to informational privacy, and, if what information about myself I comfortably share with others depend on my personality, and this in turn affect how I choose to present myself, I cannot see how the motives for collecting is significant if the collected information is information I am not comfortable with sharing. In my opinion, Rössler's need for involving motives as a differentiating factor, is because she identifies informational privacy as the conflicting interest of "wanting to hide" to that of "wanting to know" (Rössler, 2005, p. 126), and, by that, the right to informational privacy is taken as an opponent to the established civil liberties "[…] to look at the world – out of curiosity – as an when [one] want to, and to tell other's that they do so as and when they want to […]" (Rössler, 2005, p. 125). By conceiving personal information only as a source of knowledge about someone, that is, as a part of the world that people have "the right and the liberty to look at", and not conceiving personal information as a constitutive part of the person itself, both Rössler and Benn must proceed to justify informational privacy in a roundabout way. Informational privacy is only ascribed conditional or *indirect* value, leaving any value of informational privacy contingent upon its contribution to autonomy.

According to Benn (1988) and Rössler (2005), the right to privacy, by definition, restricts another's right to observe. Since the right to observe is grounded on fundamental liberties, the *onus* of justification, *prima facie,* rests on the one who will restrict or control observation. Rössler (2005, pp. 125-126), therefore, argues that a normative principle upon which a right to informational privacy is based, must be grounded in equally fundamental values, if it is not to be constantly cancelled by overriding rights. In order to constitute an equal fundamental right, not readily overridden by more basic rights, informational privacy must originate from the "[…] idea of the autonomy of the person or of respect for her identity" (Rössler, 2005, p. 126). If a restriction on observing can be justified by the

fundamental value of autonomy, then the information collected by motives or intentions incompatible with this value cannot be legitimate. On the other hand, any intentions compatible with this value is legitimate, and such motives legitimate collection of personal data or information (Rössler, 2005, pp. 124-125). Although Benn and Rössler argue for informational privacy rights grounded on the value of autonomy, neither of them think of autonomy as sufficient for specifying the content of informational privacy rights. Rössler argues that the criteria for what information is to be worthy of protection is to be specified by well-founded normative horizons of expectations relative to social norms and conventions (2005, p. 118). Benn argues similarly that

> [t]he liberal cannot give absolute specifications, however, for what is private and what is not, because privacy is context relative. I do not mean that standards differ between cultures. That is also true, but it is a different kind of relativity. Within the one culture the same matter may count as private or not, relative to the social nexus in which it is embedded (Benn, 1988, p. 268).

As previously mentioned, my objection to Benn and Rössler's accounts of informational privacy does not rest on a disagreement about the value of autonomy, but since autonomy can only provide for a minimal right to privacy (Benn, 1984, p. 224), grounding informational privacy on the value of autonomy, rather than on the value of 'personal' information as such, the right to informational privacy is fundamental only in a roundabout way via the fundamental value of autonomy. As argued by both Benn and Rössler, autonomy in itself is not sufficient for specifying the content of what is to count as information worthy of protection. For this purpose, autonomy requires established social norms and conventions. This means that a normative theory of informational privacy grounded on the value of autonomy, will not, within an environment without any established norms or conventions, be capable of providing the sufficient moral criteria necessary for determining what information can be legitimately taken and distributed by others. Also, which will become evident below, a theory that bases informational privacy rights on autonomy, in an environment in which not only the subjects but also their interactions take a different form from that of which the value of autonomy is related to, are shown inadequate, both in their foundation, and in their lack of ability to provide for specific moral criteria for what information is to count as worthy of protection in that environment.

With the development in ICTs we are all forced into a different informational environment as different entities with different interaction patterns than that of which we are

accustomed to. Colburn and Shute (2010, pp. 97-98) point out that computer science is distinguished from other sciences in that computer science, contrary to all other sciences, "creates its own subject matter". Programs, algorithms, and, data structures are, in the digital informational environment, not subject to physical, but only to logical constraints. The difference being that while social sciences observe and explain already existing patterns of behaviour in well defined corporeal objects (or subjects), computer science creates both new objects and their patterns of behaviour, or more precisely, computer science both *creates* and *studies* "[…] procedures, data types, active objects, and the virtual machines that manipulate them" (Colburn and Shute, 2010, p. 98). The computational worlds, in which we increasingly interact through new ICTs, are "[…] the products of programmers' creative imaginations […]" (Colburn and Shute, 2010, p. 98). The regions of the informational environment in which we increasingly interact as informational entities or persons, are created or engineered by computer scientists whose objective is the creation and manipulation of interaction patterns between the abstract informational entities occupying the environment (Colburn and Shute, 2010, p. 99; 2011, p. 246). For instance

> [s]ocial networking is set to undergo [a] transformation with billions of interconnected objects […] where individual 'things' in the house [such as washing machines, refrigerators, bathroom scales, etc.] can periodically tweet readings which can be easily followed from anywhere creating a *tweetOT* (Gubbi, et al., 2013, p. 1650, italics in the original, my insertions)

The objects or entities interacting within this environment are, in the same manner as the processors, computational abstractions, and represent anything from registers, memory locations, programme instructions, numbers, and procedures, to telephone books, calendars, and humans (Colburn and Shute, 2011, p. 248-249). Since the information technologies available share their ontology with their objects to the effect of a "[…] fundamental convergence between digital resources and digital tools […] there is no longer any substantial difference between the processor and the processed and the digital deals effortlessly and seamlessly with the digital" (Floridi, 2005, p. 188). This enables "[…] devices, which are normally not computers, to communicate with one another through a data network so that the network itself is not limited to the traditional structure of a computer network, but extends to ordinary things, even the human body" (Hongladarom, 2011, p. 360-361). With this, our environment can be (and increasingly is) transformed into a "smart environment" that is, a "[…] physical world that is richly and interwoven with sensors, actuators, displays, and

computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network" (Weiser quoted in Gubbi, et al., 2013 p. 1646). By being connected through a (exhaustive) continuous network, individual devices can communicate with any other device in the world. A person can for example be integrated into a (exhaustive) computer network through body area sensors that monitor physical states of the body, and smartphones or smart watches used for communication along with interfaces such as Bluetooth for interfacing the sensors (Gubbi, et al., 2013, p. 1650).

Thus, with the digital informational environment "the rule of the game" so to speak has changed in that both the nature of the entities inhabiting it and their patterns of interaction in this environment are drastically different from those on which the aforementioned liberal theories of Benn and Rössler are based. The entities assumed or presupposed by Benn and Rössler as the basis for their theories are autarchic, or autonomous and authentic concrete, non-informational entities with a right to *control* others' access to their own personal information. The informational environments such entities can adequately operate within, in relation to informational privacy concerns, are physically enclosed environments in which the person's ability to control others' access is achievable. Such environments, due to being subject to physical constraints on access, storing, and distribution, can, at least to a certain degree, "naturally" accommodate the autonomous person's informational privacy needs. On the other hand, the digital informational environment and its inhabitants or objects are constructed so as to accommodate the information technologies available, rather than the "natural" person mentioned above. By being integrated into this environment the "natural" encapsulation of information of the multi-agent system i.e. person provided by the three membranes (the corporeal, cognitive, and consciousness) is diminished to the effect of the informational person within this environment lacking "natural" protection against improper manipulation.

Although, as argued by Floridi (among others)[29], computer technology or ICTs may provide (at least part of) the solution to the problems concerning information privacy raised by the technologies in question, as individuals we lack the knowledge required for utilizing the technological means necessary for adequately controlling external access to our personal information. As pointed out by Roux and Falgoust:

---

[29] Floridi (2005) suggests problems involving information privacy to be solved by creating ontological friction within the informational environment, while Chinese walls between spheres of access is suggested by Wiegel, Van den Hoven, and Lokhorst (2005).

> While a citizen with a fair amount of knowledge about computers and smart devices may be more aware of the channels of information made available by a smart device, she still has no control over how applications cache data, and not all applications allow the user to manually clear the cache. The "walled garden" approach taken by the major smart phone software developers inhibits one's ability to write more privacy-aware applications. In some instances, a user is simply forced to use an application or forgo the capability (Roux and Falgoust, 2013, p. 189).

We are thus dependent, to a greater extent, on the mercy of others when it comes to securing our informational privacy than what informational privacy rights as control rights take into account. That is, we are to greater extent dependent on our moral status (as informational objects) in regards to informational privacy rights when this environment is rapidly becoming our most important venue of interaction.

Considering the impact the developments of new ICTs has on our lives, in order to provide for an appropriate analysis of the moral implications that might follow this development, an informational normative framework therefore must be in place. A normative framework, or normative horizons of expectation, will not do, if the normative framework does not involve an adequate concept of its subject. Since the subject is sets of information, the normative framework, through which informational privacy concerns is to be considered, must be a normative framework that recognizes the moral standing of personal information. By adopting an informational framework for informational privacy, when informational privacy rights are the protection of personhood, we will realize that personal information in itself is worthy of protection. When personal information is considered as constitutive of the person, a *direct* or fundamental value of informational privacy is provided for, and precise criteria for what information is to count as worthy of protection can be given independently of social norms and conventions.

As mentioned above, my objection to Benn and Rössler's accounts of informational privacy does not stem from a disagreement about the fundamental value of autonomy. I rather recognize and sympathize with their concern over the harmful consequences caused by free access to personal information as valid reasons for promoting and defending informational privacy rights. Nevertheless, in my opinion, grounding these rights on the value of autonomy is insufficient. The "minimalness" of the right to informational privacy provided by the value of autonomy can be remedied by adequate social norms and conventions. In view, however, of the development of new ICTs, and the peculiarity of the accommodating informational environment, by virtue of which, both its entities and their forms of interactions takes a

different form from those presupposed by conventional theories of informational privacy, and the increasing impact these new technologies has on our everyday lives, a revision of the value of personal information, in order to determine obligatory constraints on informational behaviour or interaction is called for.

4.2 On the Distinction Between the Natural and the Informational Person in Relation to Moral Status

Above, I have argued that the distinction between the person and her information is mistaken. I argued that personal information should not be separated from the moral (human) agent to the effect of personal information being ascribed moral status. In justification of this claim I argued for a conceptual revision of the conventional, liberal conception of personhood as autonomy, to a new conception of personhood as the right degree of detachment and unification of personal information. In order to make the new concept more intuitive it will be appropriate to outline more clearly the distinction between the natural[30] and informational person as a distinction in LoA. This distinction in LoA will then be suggested as a solution to the objection, articulated by Himma (2004), that the person, as a set of information, is an abstract object and thus cannot be identical with the natural person. Since personal information is only referring to the natural person who defines the set of information in question, any moral status ascribed the natural person cannot as such be extended to the informational person, Himma argues (2004, pp. 147-148). The distinction in LoA will then be used to elucidate the above claim of the need for an informational LoA as the normative framework relating to informational privacy, and serve as a preliminary argument for a justification of personal information having *direct* value, suggested in the beginning of this chapter, which in turn will make the right to informational privacy more adequate as a robust protection of personal information.

Himma (2004, pp. 147-148) raised the objection[31], that since a particular natural

[30] 'Natural person' here meaning the *concrete* individual human being (without taking into consideration any specific concept of personhood).

[31] Himma (2004) is not taking part in the discussion of informational privacy in raising this objection; the objection is raised against the claim of information in itself (whether personal or not) having intrinsic value.

person, Mary, *qua* the human agent herself, and the person, Mary, *qua* information object cannot be identical, it is not obvious that these two are morally analogous. Himma says that:

> To say that a particular person, Mary, can be "modelled" or "analysed" as an information object is, then, to say that there exists a set of propositions that contain a description of the various states, properties, and attributes of Mary over time and a collection of functions defining Mary's reactions, behaviors, etc. *Qua* human being, Mary is a collection of molecules arranged in a particular way that function in various self-sustaining ways; *qua* information object, the human being Mary is described by the set of propositions and functions that constitute an information object. Strictly speaking, then, the entity we refer to as "Mary" *defines* an abstract information object, but is not *identical* with that object (Himma, 2004, p. 148).

From this it should be obvious that the natural person, Mary^{n}, and the informational person, Mary^{i}, cannot be one and the same object or entity, and thus, any moral status ascribed to the former cannot, as such, be extended to the latter. According to Himma, to have moral standing or status, and by that being a moral entity, is to be owed at least one direct duty. A direct duty is a duty that "[…] immediately concerns the being to whom the duty is owed [while an indirect duty] immediately concerns the treatment of something other than the subject to whom the duty is owed […] (Himma, 2004, p. 145, my insertion). According to this, I take it that, since Himma sees personal information as only describing, or referring to, the person, the person at best is owed by others only an indirect duty in their treatment of her information. Because their treatment of her information immediately concerns the treatment of something other than the subject to whom the duty is owed, the person, as information object, is dependent on the natural person (to whom the information object refers) and her moral status in order to be taken into moral considerations. As Himma (2004, p. 145, footnote 2) points out, to merely be "*morally considerable"* in relation to the well-being of the moral entity (i.e. the natural person) is a much weaker claim that that of claiming the direct duty of others. As Himma states:

> My right to life, for example, is constituted in part certain obligatory constraints on the behavior of other moral agents; in particular, others are constrained from intentionally killing me unless I am culpably posing a threat of death or grievous bodily harm to some other right holder [something] that is merely *morally considerable* has only a right to its well being taken into *consideration* in the deliberations of moral agents (Himma, 2004, p. 145, footnote 2, my insertion, last italics mine).

Others' indirect duties towards you are not obligatory and thus easily overridden by other interests. By considering personal information as only referential, and thus only to be taken indirectly, via the moral status of the natural person, into consideration of (moral) obligations, informational privacy rights are easily overridden by other moral rights defined by claims on direct duty. On this account personal information can only have moral value via an agent with moral status (whatever property this status is based upon) whereas the agent has intrinsic value by virtue of having the property in question, and is thus beneficiary of direct duties. Therefore, even a *potential* threat to someone's (moral) right, or, in terms of Rössler, established civil rights, can be taken as reasons for overriding claims on informational privacy.

In what follows, I will provide an argument in opposition to this line of thought, by acknowledging the *direct* value of personal information and by showing the natural person and the informational person as a unity of moral status. Once this is acknowledged it will become evident that by treating (a specific kind or set of) information, one is directly treating the moral agent herself, and this opens up for determining obligatory (moral) duties of informational behaviour appropriate of the digital informational environment.

In Chapter 3, I argued for an informational conception of the person developed by Floridi (2011) where the person is to be conceived of as a multi-agent system consisting of three membranes of encapsulated information and informational processes, loosely combined as one network. As will be explained shortly, I take consciousness to be the capacity to store, interpret, and repurpose data and/or information in order to create or construct a unification of the multi-agent system's three membranes or agents, to the effect of constructing for itself a separateness or detachment from the world. Bawden argues that:

> […] with life we find the emergence of meaning and context. The genetic code, for example, allows a particular triplet of DNA bases to have the meaning that a particular amino acid is to be added to a protein under construction, but only in the context of the cell nucleus […] Further, it has become clear that the origin of life itself may best be viewed as an "information event", as is the subsequent evolution of all life, and the development of intelligence and culture […] The crucial aspect is not the arrangement of materials to form the autonomy of a living creature, nor the metabolic processes; rather it is the initiation of information storage and communication between generations that marks the origin of life […]" (Bawden, 2007, p. 315-316).

According to this the crucial feature of life is the capacity to store information. If informational processes or capacities such as the capacity to store information are crucial, then, since as mentioned above information is what activates these processes, the information

stored must play an equally important part in forming the person in question. Recalling Himma's claim that the moral status of the natural person cannot be extended, as such, to the informational person, if views such as Bawden's are at all plausible, that is, if the crucial aspect of forming the person, Mary, not necessarily is that of the arrangements of materials, or, in terms of Himma, molecules, but informational processes such as storing of information and communication, why should Mary *qua* molecules arranged in a particular way have moral status whilst Mary *qua* information object does not have moral status?

On the other hand, Himma, by emphasizing that Mary *qua* human being is to be understood as the "[…] collection of molecules *arranged* in a *particular* way […]" (2004, p. 148) he seems to be suggesting that it is the patterns of the molecules not the molecules themselves that is the identifying property of Mary. On the other hand, the same arrangement or "patterns of organization" [32] can be interpreted as Mary *qua* information object. Recall, from Chapter 3, information object being that of data-structures and their behaviours bundled together in one object of information (Floridi, 2002, p. 288). The patterns of Mary *qua* a collection of particularly arranged molecules and Mary *qua* a collection of data structures, are identically organized but interpreted at different LoAs. That is, $Mary^{n}$ and $Mary^{i}$ are two variant understandings of $Mary^{S}$ (the system)[33]. Even though one understanding of $Mary^{S}$ is abstract and the other is concrete, they are identical to $Mary^{S}$ in that it is not (necessarily) the "physical" properties (or lack thereof) of $Mary^{S}$ that are her identifying properties, but her unique "patterns of organization" i.e. her unique information patterns. Himma is mistaken in assuming $Mary^{n}$ as $Mary^{S}$ and thus in making the moral status of $Mary^{i}$ a question of identity between $Mary^{n}$ and $Mary^{i}$ when it should be a question of the identity between $Mary^{n}$ and $Mary^{S}$ and $Mary^{i}$ and $Mary^{S}$, where the moral status of $Mary^{i}$ is due to her being identical to $Mary^{S}$.

As mentioned in Chapter 3, Floridi defines LoAs (Level of Abstraction) as frameworks through which an observer interacts with the world. Any object or system can be described at a range of LoAs. The observer's LoA(s), which are adjusted and attuned

---

[32] Recall from Chapter 3, Bates (2006) defines information as "patterns of organization," in order to emphasize the all inclusiveness of the concept of information. That is, a definition of information as patterns of organization is to include "[…] every physical, biological, perceptual, and cognitive pattern of organization that exists or is extracted by sensing beings [as well as including] the physical and biological patterns of organization not sensed by us […] from the atomic to the galactic, from the virus to the ecosystem" (Bates, 2006, p. 1035).

[33] I have here been drawing on Bates (2005) who argues that although information exists independently of the experience of living creatures, there can be many equally true variant understandings of the same structure. A variant of this view, in terms of Floridi (2013, pp. 29-52) will be explained and adopted shortly.

according to the observer's interests, values etc., determines which properties of the observed system is given attention by the observer (Floridi, 2013, pp. 30-31). To each LoA is a corresponding set of available observables[34], or typed, interpreted variables. A typed variable is, according to Floridi, "[…] a variable qualified to hold only a declared *kind* of data" (2013, p. 31). Typed variables are interpreted when they come together with a statement of what feature of the system the observable represents. For example, a set of data could have *natural numbers* as its type and *bank account* as a feature or function of the system. The higher the LoA the more properties of the observed object or system are eliminated or lost to the observer, that is, the higher the observer's LoA of the observed, the smaller the set of observables available to the observer. The lower the LoA, the larger set of observables available to the observer, and the more detailed analysis of the system. Depending on LoA, any object, i.e. system can be observed and examined (Floridi, 2013, pp. 29-34). At the informational LoA^{i} the system being analysed is

> […] considered and treated as discrete, self-contained, encapsulated packages containing: […] the appropriate data structures, which constitute the nature of the entity in question: the current state of the object, its unique identity, and attributes; and […] a collection of operations, or procedures (*methods)*, which are activated (invoked) by various interactions of stimuli, namely messages received from other objects or changes within itself and which correspondingly define how the system behaves or reacts to them (Floridi, 2013, pp. 105-106, italics in the original)

Each LoA, through which the system is examined or observed, can provide a determinate analysis with a resulting model of the system in question (Floridi, 2013, p. 31). The system itself, however, is independent of any LoA.

On an informational view of the person, the self is located as information and informational processes in the brain (Floridi, 2011, pp. 561-562). I suggest that the self is present, however, as a cohesive unity of experiences, subjectively interpreted by the multi-agent system in question, in order, in terms of Collier, to "[…] modify itself and its environment to enhance its survival, responding to both environmental and internal stimuli to modify its basic functions to increase its viability" (2004, p. 164). The self is the set of interpreted (and repurposed) core or nucleus information, unified and constructed into a coherent set of propositions or semantic information. This information is of *direct* value to

[34] As emphasized by Floridi (2013, p. 31) the term 'observable' is not to be confused with 'empirically perceivable', as the examined system need not be concrete but could be entirely abstract.

the multi-agent system in relation to constructing the subsystems into one system. By optimizing its behavioural unity, the system as a whole is able to maintain stability. Or in terms of Dennett: "Our component modules have to act in opportunistic but amazingly resourceful ways to produce a modicum of behavioral unity, *which is then enhanced by [a] greater unity*" (1992, italics in original, my insertion). This greater unity, which enhances our behavioural unity, is due to our detachment or separation from the world, which in turn, determines the conditions under which the *self* will resist both internally and externally generated disruptive forces[35], providing the conditions for stability or mental homeostasis. On, the other hand, however, many models can be made of the system, making it prone to improper manipulations, to the effect of de-stabilizing the system.

As mentioned above, according to Floridi, a LoA is a specific set of typed observables through which the observer accesses and interacts with the environment (Floridi, 2013, p. 41). By its utilization of semantic information in order to interpret and construct a stable unity of itself, the multi-agent system is detaching itself from the world, that is, the informational person does not stand in a direct relation with the world, but indirectly by interpretation. This results in the self, or the cohesive or coherent unity of the multi-agent system, not standing in direct relation to itself, the self never seeing the full picture of its system.

According to an informational conceptual framework, data is primary, that is, "in the beginning were the data" (Floridi, 2010b, p. 275). At the informational LoA then, the person is primarily "[…] a data–structure"–an "informational object"–composed of […] "relations" describable as "mind independent points of lack of uniformity"" (Floridi in Bynum, 2010, p. 184). This means that, conceptually, at the informational LoA, the person, i.e. the multi-agent system, is primarily data. For instance, the emotional states of Mary^{S} (as data structure) can be described as minute changes or lacks of uniformity in Mary^{S}'s (in terms of Parker, 1974, quoted in Bates, 2006, p. 1033) "patterns of organization of matter and energy". Minute changes of conductance across the surface of the skin of Mary^{S}, initiated by her autonomic nervous system (both of which also describable as points of differences or "patterns of energy and matter"), can be taken as measurements of arousal and valence (which, by many scientists is taken as the main dimension of emotions) (Fletcher, et al., 2010). Mary^{S} can then, due to being endowed with a capacity of interpretation, by information and

[35] According to Collier, cohesion " […] determines the condition under which something will resist both externally and internally generated disruptive forces, giving the conditions for stability (2004, p. 156).

informational processes encapsulated within her cognitive and consciousness membranes, create emotional representations and semantic information from this data, for example, represented as a feeling of anxiety, interpreted as being afraid of the dark[36]. This allows Mary^S to create a cohesive unification of the system, in that Mary^S can use her data structure to create a model of herself as a system that is afraid of the dark, and, by that, make the system into a behavioural unity, in order to take appropriate action when placed in relevant (dark) conditions. Since, however, semantic information requires a capacity to "[…] interpret something as something else" (Floridi, 2010b, p. 276), a distance between the multi-agent system and the world is created, to the effect that the relation between data and information is not exhaustive but interpreted through LoA(s). This on the other hand, leaves the system vulnerable, in its unification, to external interpretations or models of itself, which in turn, may give rise to instability in the system.

On the conventional (liberal) accounts of informational privacy personal information is taken to only be referring to and not as constitutive parts of the person. On the other hand, on the proposed informational account, "personal information" is related or connected to the data structures, i.e. multi-agent system (in that this information is extracted from the data structures), but are at the same time the constitutive parts of the models of the multi-agent system in question. That is, the system uses its own (personal) information in its analysis of itself with the resulting model. The system's own model or *self* can be manipulated by external models of the system because the system's data structures are not transparent to the system (i.e. itself). Personal information is constitutive parts of the models connected to the system, the system itself being beyond its own reach. Distribution of a system's personal information is thus distribution of the (informational) person since the distribution of this information results in a manipulation of the model, by the external construction of new models, to the effect of a reconstruction of the self.

We are treating the person when treating her information because this information as well as any treatment of that information is what is constructing her. Because of this, by taking and using the system's personal information, one is at the same time manipulating the model of the system i.e. its *self*, which can undermine or damage the stability of the system. If Mary^S is not transparent to herself or Mary^i (nor anyone else), and by that allowing for a

[36] As noted by Bawden (2007, footnote 15) (human or semantic) information in information theory is often equated with some composite of data and meaning. Whether semantic information is strictly reducible to data is not of concern in this context. See Vakarelov (2010), and Floridi (2010b) for a discussion.

variety of equally "good" or appropriate interpretations or models of Mary^{S}, then Mary^{i} can be conceived of as the sum of all these models[37]. If *Mary*^{i} is the sum of all her models, then, any "model-making" of Mary^{S} is a manipulation of Mary^{i}, since every model constructed of Mary^{S} results in a reconstruction of Mary^{i}. Mary^{S}, however, is depending on stable self-modelling in order to optimize her functioning as a distributed system (that is, Mary^{S} is depending on stable model-making for securing the behavioural unity of her components or parts). Too extensive external *Mary-modelling* would disturb the unity of Mary^{S} by effectuating unlimited manipulation of the information constituting Mary^{i}, to the effect of risking informational fragmentation of Mary^{i}, and by that jeopardizing the behavioural unity of the components of the system Mary. For instance Mary could be fitted with wearable devices, such as wristbands, that monitor Mary's emotional states by detecting minute changes in the electrical conductivity and temperature of Mary's skin that are driven by Mary's autonomic nervous system which functions largely below the level of consciousness. The wearable device can thus read emotional states of Mary that Mary did not know she was in. Mary could have constructed a *confident-model* of herself, while the device is constructing an *anxious-model* of Mary, the two contradicting models disrupting the behavioural unity of Mary in that, in order to function adequately, Mary might have disregarded the information (encapsulated within the corporeal membrane) whilst analysing her system[38]. Since on this (the informational) view, the *self* is a connection between data structure and interpretations of these data structures (i.e. information), I suggest that, if, conceptually, the multi-agent system primarily is encapsulated data, then, normatively, every individual piece of personal information is, on its own or in combination, a constitutive part of a self-unifying (coherent and distinctively characteristic) whole, in that this information is used by the multi-agent system to interpret and/or construct a coherent unity in order to maintain stability of the multi-agent system and by that sustaining the system, personal information thus having direct value to its connected system.

---

[37] According to Floridi, since the ultimate reality is inaccessible to us and our understanding of it is achieved by us constructing models, through various LoA, of the information it provides and the constraints it places upon our experiences, the experienced world is limited to the sum total of our models (Floridi in Bynum, 2010, p. 183).

[38] Professor Picard has lead a team at MIT Media Lab, pioneering research in developing 'affective wearables', that is, wearable systems, equipped with biosensors such as wrists sensors and tools (such as a smartphone application) that detects changes in the activity of the wearer's autonomic nervous system. These changes or patterns can be interpreted as representations of the wearer's affective patterns or emotional states. These devices allow for long-term continuous data gathering in order to help individual understand and communicate their internal state changes. For reference see Fletcher, et al. (2010); and Hernandez, et al. (2013).

Above I argued for the inadequacy of theories not recognizing the direct value of personal information, treating personal information as something separate of the person, leaving it to the context in which the information is collected to determine the moral value of such information. In the digital environment, however, all that there is, is data or information, and interactions within this environment become interpretable as access/alter or read/write activities (Floridi, 2005, p. 189). That is, interaction, within the digital environment, can be interpreted as requests for information and alterations of data, and it takes form of a seamless flow of information between informational agents or entities, all of which are created or constructed by computer engineers. To conclude this section, I will argue that within the digital informational environment, by Rössler's account of informational privacy one risks ending up with standards for informational interaction that are disharmonious with the liberal tradition. This claim will be exemplified by making use of Wiegel, Van den Hoven, and Lokhorst (2005) approach to model moral constraints on interaction within the digital informational environment[39].

Wiegel, Van den Hoven, and Lokhorst are looking to develop an approach on how to model interaction patterns within the digital informational environment that maintains informational privacy, by defining information (conceived of as a cluster of data structures) itself as an agent "[…] with desires, intentions and beliefs about its environment that is able to act" (Wiegel, Van den Hoven and Lokhorst, 2005, p. 253). The informational agent's aims are to maintain data integrity,[40] provide rightful access, and inform all those (agents) it is obligated to inform (Wiegel, Van den Hoven, and Lokhorst, 2005, p. 253). Whilst conceptualizing information itself as an agent with the capacity to interact with its environment, Wiegel, Van den Hoven, and Lokhorst do not recognize the person as this informational agent. The moral criteria for informational interaction, that is, the criteria for what can be rightfully accessed or altered by what informational agent is not the direct value of personal information, but the relation between attributes of the requested information, the requesting agent's role, and the extent of which the requiring agent's role is assigned both to the sphere in which the requested information originated, and its sphere of intended use. Data integrity is maintained by restricting distribution and use of information to and within

[39] Although not mentioning autonomy as a justifying value, this approach is compatible with the liberal accounts considered above when looking to construct interaction patterns in a digital informational environment that maintains the "concrete" person's informational privacy.

[40] I assume that what is meant by integrity in this context is just that of keeping data from improper alterations (Brazier et al., 2004, p. 19-20).

domains defined by the spheres attached to the particular role of the information i.e. agent, as either data-subject (personal data and/or information), data-administrator (data manipulator), or stakeholder, operating within the domain in question. The spheres specify the particular value or purpose of their information by being defined according to need and custom. To prevent the use of a particular good with the purpose of gaining dominance in a different sphere, the information gained in a particular sphere cannot be used for a purpose other than the purpose specified in this particular sphere. The separate spheres make up the informational society or environment within which the informational agents interact. As a general rule, information assigned the role of data-subject has the right to access and distribute its own data (Wiegel, Van den Hoven, and Lokhorst, 2005, pp. 253-255). By this I take the information as data-subject to have unrestricted access and distributions rights. On the other hand, the data-subject does not have the right to change its own data as this right belongs to a data-administrator. In addition to unrestricted access and distribution rights, the data-subject also has an obligation to distribute information requested by data-administrators and stakeholders within its "intended application domain." The data-administrator, on the other hand, is responsible for the correctness of the data in question and has obligations to alter data in accordance with the restrictions accompanying its role and domain (Wiegel, Van den Hoven, and Lokhorst, 2005, pp. 253-255).

Rössler, as mentioned in section 4.1, argues that, in order to determine when what data becomes worthy of protection and when it is legitimately accessed, one has to look, through a normative horizon of expectations (guaranteeing civil liberties), at the contexts of when data protection becomes significant (Rössler, 2005, p. 119, 124). Van den Hoven states similarly, that "[t]he […] value of information is local and allocation schemes and local practices that distribute access to information should accommodate local *meanings* and should, therefore, be associated with specific spheres" (2008, pp. 314, italics in the original). Violations of privacy is "[…] construed as the morally impropriate transfer of personal data across the boundaries of what we intuitively think of as separate […] spheres of access" (Van den Hoven, 2008, pp. 314). Similarly, Rössler argues that the capturing, collecting, and storing of personal data or information, by state institutions, concerning an individual person is not in itself a bad thing. On the contrary, the idea of individual rights and the possibility of making claims according to such rights, naturally and necessarily entail the identification of individuals. Such activity, by state institutions, can be the endeavour, by the state, to achieve equality among its citizens. Such activity, however, according to Rössler, gives rise to the

danger of shifting personal information from one context to another and by that permitting new classifications that may lead to discriminations against the person thus classified (Rössler, 2005, p. 126). In both of the above accounts, the legitimacy of the motives is what justifies access and collection. On these accounts, it is not the kind of information, i.e. the kind of information that has a direct moral relevance in relation to a specific, informational person (or in other words personal information) as such, but the context in which this information is accessed, which determines the value of, or the right to, informational privacy.[41]

Contrary to Benn and Rössler's accounts of informational privacy, Wiegel, Van den Hoven and Lokhorst's (2005) "approach to modelling moral constraints in complex informational relationships" does not make any reference to the value of autonomy. Where personal information is seen as the separate passive product of an autonomous person in Benn and Rössler's accounts of informational privacy, the same approach can be said to represent the flip side of the coin also, in that it seems to result in some sort of informational outsourcing. The (autonomous) human agent is left passive, separated from its information, which seems to be living its own life through patterns of informational interaction constructed by computer scientists or engineers. Personal information is, within the informational environment constructed by Wiegel, Van den Hoven and Lokhorst (2005), assigned the role of data-subject with unrestricted access and distribution rights to/of its data, within the sphere of interests it is allocated to. Since distribution and access is constrained to and within separate spheres, the human agent is able to estimate who has what information about her. Her expectations concerning what knowledge others have about her are secured from inaccuracy by preventing transference of data, of the data subject, to a different sphere, and by the data-administrator's obligation to inform the data-subject of any changes it makes to the data (-subject). The human agent, through her representative data-subject i.e. personal information, thus controls, or rather, has an opportunity to monitor, what other people know about her and who those agents are to which its information is distributed (by knowing their representative agent's roles as either data-subject, data-administrator or stakeholder). The "natural" person's informational privacy is maintained by separating personal information from the person and containing this information safely within the sphere it is allocated to. The person's autonomy in self-presentation is intact since the strict containment of the

[41] On Rössler's account the context must be in accordance with autonomy (2005, pp. 119-129), while Wiegel, Van den Hoven, and Lokhorst (2005) makes no reference to the value of autonomy.

information within the spheres, preserves the person's undisrupted well-defined normative horizons of expectation of what others might know about her, that, according to Rössler (2005, p. 114), is "necessary for the exercise of autonomy".

In Wiegel, Van den Hoven, and Lokhorst's (2005) approach to modelling moral constraints in informational interactions, we are, in the digital informational environment, existing as more or less free floating fragmented informational objects or agents. "Natural" encapsulation of information is eliminated and because of this elimination of encapsulation, access is unrestricted. The unlimited access is then remedied by the encapsulation of personal information on a criterion of "spheres of justice" or "spheres of access" such as spheres of national security, medical interests, etc., and not on a criterion of self-unification. Considering that our interactions increasingly take place within the digital environment, which perhaps (in the future) is to become the main arena for human interaction, on this approach, by not considering our informational unity and self-unification as morally relevant in creating the digital environment, the moral principles by which to constrain interaction, in (potentially) our main arena of interaction, are to be based on a conception of personal information as a mere resource. With the moral criterion for informational interaction being that of fair or just distribution of social goods, and not the informational integrity of the person, we (as personal information) are to be considered as the means for such distribution. This, although perhaps compatible with the liberal conception of informational privacy as the right to control access, seems nevertheless at odds with the liberal tradition of the integrity of the person of never letting oneself be used as a mere means. If, on the other hand, the informational environment was to be constructed on a moral criterion grounded on the direct value of personal information in relation to the informational person, and thus on the right to informational integrity, moral principles for informational interaction will be more in tune with the liberal tradition.

4.3 The Inverse Function as the "Determinator" of Personal Information

In the previous section, I argued for the moral status of the informational person by showing that the distinction between the natural and informational person is a matter of difference in LoAs and not a difference in properties. The moral status (of being a moral entity, that is, an

entity owed respect) ascribed one, can thus be ascribed the other. Moral status should be extended to the informational person when the *direct* value of personal information is recognized. Personal information has a direct value in relation to the multi-agent system, in that each individual piece of information that is a member of the unique set of the system in question is used by the multi-agent system to construct an informative and coherent unity, consistent with its data-structure, in order to maintain stability. Personal information thus has *direct* value for the system in being a constitutive and stabilizing part of a self-unifying whole.

In section 4.1, I argued that, in order to provide for adequate criteria for the content of informational privacy rights, due to the fact that informational interactions to a greater and greater extent take place within the informational environment by means of new ICTs, informational privacy rights must be grounded on the *direct* or fundamental value of personal information in relation to the stability of the multi-agent system, rather than via the fundamental value of autonomy. As mentioned at the beginning of this chapter, by a *core* or *nucleus* set of information, I mean that information that could not be constitutive of another set, that is, that information, either as a single piece of information or in combination, that is unique to a particular informational person. In this section, I will give an account for how the content of the *core* or *nucleus* set of information is to be determined, or in other words, how to determine what is to count as personal information. This set will be established as the centre of the system's self-unification.

In order to determine the content of the nucleus set of information of an informational person I will argue in favour of, and elaborate on, Floridi's (2013, p. 311) suggestion of the inverse function in determining what information is constitutive of the person. I will begin with bringing in the account of Al-Fedaghi (2005) on how personal or (in terms of Al-Fedaghi) private information is to be calculated. This account is in line with conventional theories, including those of Benn and Rössler, in that what is being considered as the essential property of personal or private information is its referring role. When reference is considered determinant of personal information, the information that counts as personal information is too comprehensive and additional conditions is required for determining its value. The advantage of the inverse function is that it excludes any contingent or peripheral information and personal information is limited to that information that is of direct value to the informational person, the problems that arise due to trivial information being included as personal information in considerations of informational privacy rights, are thus avoided.

Al-Fedaghi (2005)[42], in developing a "theoretical formalism to specify private information", suggests a set theoretic approach in order to determine or calculate what information is to count as personal or, in terms of Al-Fedaghi, private information. According to Al-Fedaghi (2005), by utilizing "[…] single-referent linguistic assertions in defining "private information" in terms of 'atomicity' and identification […]", a person's atomic private information, or private assertions (assertions with *one* recognizable referent), is recognized and the person's private information can then be calculated. For example, 'Mary has brown eyes' is an atomic private assertion of Mary and thus private information. 'Mary and John are brother and sister and both have brown eyes' is a compound private information assertion but can be reduced to 'Mary has brown eyes', 'Mary has a brother', 'Mary is a sister', 'John has brown eyes', and so on. The set of private information can thus be defined as "[…] the set of every assertion that has a single referent that signifies a single individual [person]" (Al-Fedaghi, 2005, my insertion). The subsets of this set being

> […] the set of pieces of atomic private information of an individual [this set in turn having as its subsets] the set of pieces of atomic private information that is in the possession of others [and] the set of pieces of atomic private information that is only known by the proprietor [and] the set of pieces of private information of other individuals that is in the possession of an individual, however, he/she is not its proprietor" (Al-Fedaghi, 2005, my insertions).

According to the above, the strict measure of what is private information is *identifiability.* Al-Fedaghi, however, recognizes that this notion of private information is too encompassing in determining what information is to count as worthy of protection, in that most of the information included in a person's set of private information is ordinary and trivial (Al-Fedaghi, 2005; 2006). Al-Fedaghi is thus forced to introduce a sensitivity condition of private information. The term 'private information sensitivity' expresses, according to Al-Fedaghi, a notion of information sensitivity by degree, and an approach to determine its degree of 'sensitivity' or 'privacy-ness' "[…] that involves a linguistic inquiry to discover the 'tendencies' of different types of private information to ignite different levels of sensitivity" (Al-Fedaghi, 2005). I appreciate that Al-Fedaghi's theoretical formalism only is set forth as a

---

[42] In Al-Fedaghi (2005; 2006) a person's set of private information is purely referential to a natural person (a human being). Al-Fedaghi, thus, prefer the term 'private information' to 'personal information' since he understand 'personal' to imply "ownership as in personal property", while 'private information' has connotations of a distinction between proprietorship and possessor. The proprietorship of the information can be other that its possessor.

descriptive clarification of what private information is, and not as a normative or "value theory" of personal information and informational privacy. However, by claiming that "[t]he sensitivity *thresholds* of applicability are a pragmatic concern" (Al-Fedaghi, 2005) and not a theoretical one, what pieces of information are to be valued out of the totality of private information is indeterminate and dependent on additional conditions such as, for example, social and cultural norms, conventions, and interests. Al-Fedaghi's definition of private information is thus rather self-evident and of little use without also giving an account for the content of sensitive private information. What is needed is a way to isolate the core or nucleus information constitutive of the person from the trivial or periphery information only contingently relation to the person.

Floridi (2013, pp. 309-312) briefly suggests the inverse function as the determinant of what information is to count as constitutive of the person. A function represents a special kind of relation where every object *a* from the domain is related to the value of the function at *a*. That is, a function is a rule or process that assign a unique object *b* to any object *a* from the domain of the function, the value of the function at *a* (Hrbacek and Jech, 1999, p. 23). The inverse function states that for each $x \in X$, x is related to a different $y \in Y$ and for every $y \in Y$ there is an $x \in X$ such that $f(x) = y$. According to Floridi: "The obvious but powerful property that the inverse function enjoys is that of uniquely identifying the input x of another function based only on its output y, for all $y \in Y$. In plain English, a function leads you from x to y and an inverse function leads you back, from y to x" (2013, p. 311). The inverse function uniquely leads you back to the originate set, and a distinction can be made between core or nucleus information and periphery information. The set of trivial or *periphery* information of an informational person is the set of information that, either as individual pieces of information or collectively, does not signify any unique properties of the informational system in question (i.e. person). This set includes information such as: eye colour, hair colour, height, age, gender, address, phone number, name, and so on. Although the information in this set refers to the person in question, this information is either contingent or non-exclusive to the person. The *core* or *nucleus* set, on the other hand, is that information (i.e. patterns of organization) that, either as single pieces of information or in combination, is uniquely connected to a particular multi-agent system. That is, any information or patterns of organization that is, signifies, or represents some unique property of the person. Elements or information of this set include "patterns of organization" of distinct qualities, tendencies, and behaviour such as: medical records, retina patterns, DNA, life-style, belief system, interests,

etc.

As mentioned in section 4.2, what is important when it comes to an informational ontology, is arrangement or patterns of organization. In terms of Floridi "[…] we are homeostatic information patterns, bent on restricting all forms of entropy […]" (2013, p. 310). Mary^{i} is a set of patterns of organization, i.e. information, some of which are constitutive of Mary^{i}. The patterns constitutive of Mary are elements of Mary's core or nucleus set of information. The core or nucleus set of Mary is the subset, of Mary^{S,}, consisting of those elements i.e. pieces of information that constitute the distinct and characteristic patterns of organization, together called Mary. Although an output can drastically differ in representation[43] from its input, the inverse function takes you back from the patterns of organization of the output to the original patterns of organization of the input. Elements included in the nucleus set of information are thus any patterns of organization, copied in one form or another, that by the inverse function, lead back to a pattern of organization of the multi-agent system in question.

By this, I suggest the inverse function as the function for determining the content of the nucleus set of information by indicating the *information propinquity*[44] of this information in relation to its multi-agent system. *Information propinquity* indicates the constitutive function of this information. For instance, "Mary has brown eyes" is not an element of Mary^{C}, since there are probably multiple brown eyed (multi-agent) systems named Mary. On the other hand, any representation of the exact/original/unique pattern of pigments of Mary^{S}'s iris, would be an element of this set, since, by the inverse function, the pattern of organization or information of any (copied) representation would uniquely lead back to the originate set, and would thus be an element of this set. In other words, the core or nucleus set of Mary is the sum of patterns of qualities, patterns of behaviour, and patterns of tendencies that are

---

[43] By representation I will make use of Bates' (2006) definition of represented information as "natural information that is encoded or embodied". According to Bates, "[*e*]*ncoded information* is natural information that has symbolic, linguistic, and/or signal-based patterns of organization. *Embodied information* is the corporeal expression or manifestation of information previously in encoded form" (Bates, 2006, p. 1035). This is different from Floridi in that Bates considers all information as natural information, while Floridi (2010b) distinguish *semantic information* from *natural information*. As mentioned above, however, the discussion of whether or not all information are strictly reducible to natural information, is, in the present context, not crucial, what is important is that the same pattern of organization can be represented and copied in multiple forms.

[44] By Information propinquity I do not mean physical closeness, but something similar to "functional propinquity" (Korzenny, (1978) defines functional propinquity as presence across long distances in that functional propinquity is what diminish the impact of physical separation). In relation to the multi-agent system, information propinquity is what diminishes the impact of the separateness of the subsystems on the system. It is the condition for the system's self-unification, that is, information propinquity is the multi-agent system's perceived unity of its distributed subsystems.

forming the characteristic arrangement that is $Mary^{S}$. A person's name, on the other hand, is not personal or constitutive information. Collecting, copying, and/or, distributing the name 'Mary' is not to collect, copy, and/or distribute information of $Mary^{C}$ since 'Mary' does not uniquely lead back to this set but is an element of every person called or named 'Mary' Even if $Mary^{S}$ was the only multi-agent system called 'Mary', so that 'Mary' would exclusively lead back to $Mary^{Periphery}$, 'Mary' would not qualify for membership in $Mary^{C}$, because the unique relation in this case is coincidental 'Mary' is contingent to $Mary^{S}$ and is not a pattern of her distinctive qualities, behaviour, or tendencies, that is, 'Mary' is not an element of $Mary^{C}$.

The detailed patterns of a person's energy consumption; collected by smart metering systems and distributed through a digital network; could be constitutive information of the person in question. According to the European Data Protection Supervisor (EDPS)(2012), with smart meters it will be possible to read and record energy consumption with up to fifteen minutes intervals, to the effect of a significant increase in the amount of available energy consumption data. EDPS states that

> [w]ith data at such granularity, those who have access to smart metering data can know when each individual appliance in a household is turned on and off, and can often also identify what specific appliances are used. Smart meters can also provide a detailed breakdown of energy usage over a long period of time, which can show pattern of use […] deployment of smart metering may lead to tracking everyday lives of people in their own homes and building detailed profiles of all individuals based on their domestic activities […] Patterns can be tracked at the level of individual households but also for many households, taken together, aggregated, and sorted by area, demographics and so on. Profiles can thus be developed, and then applied back to individual households and individual members of those households (EDPS, 2012).

With personal or constitutive information being patterns of distinct qualities, behaviour, and tendencies, it is not, in my opinion, with regard to smart metering, unreasonable to assume that information patterns of energy consumption can uniquely correspond with information patterns i.e. patterns of organization, that constitute the energy consuming person, since it is the arrangements and not the fabric, so to speak, that make up the person. The detailed patterns of energy consumption can thus be considered as a copy of the original patterns of organization i.e. the person, whenever these patterns of organization i.e. information exclusively lead back to the originate set. Lisovich and Wicker (2008) claim that: "[…] the detailed household consumption data gathered by advanced metering projects can […] be repurposed […] to reveal personally identifying information such as an individual's

activities, preferences, and even beliefs". Accordingly, it could be possible to move, for example, from Mary's distinct qualities, tendencies, and behaviour to Mary's household energy consumption information and back to uniquely identifying such properties of Mary from this information[45], this information should thus be considered elements of the core or nucleus set of Mary^{i}. The core or nucleus set of Mary^{i}, being Mary's centre of unification by being the set of observables, through which, Mary, the multi-agent system, unify, by constructing models of herself.

4.4 The Harm in Taking Mary^{C}

As argued in section 4.2, in order to maintain stability or homeostasis of the multi-agent system, that is, to ensure the most beneficial interactions between the subsystems (i.e. between a corporeal, a cognitive, and a consciousness membrane) of the multi-agent system, the system or informational person, Mary^{i}, must engage in the self-unifying activity of interpreting her own data structures. This activity is that of making models of herself that are the results of an analysis of the multi-agent system through a first-person LoA by information and informational processes encapsulated within the three membranes (and most importantly within the consciousness membrane). By virtue of this activity, Mary^{i}, is separating or detaching herself from the world, in order to resist disruptive external forces. This separation results, however, in Mary^{i}, neither standing in a direct relation to the world, nor to herself. Thus, when "natural" encapsulation is eliminated, this separation results in the system being vulnerable to the disruptive or manipulative external forces that the separation was supposed to resist. Recall from Chapter 2 the privacy concerns relating to life-logging, where "life-log" refers to "[…] a comprehensive multimedia archive of an individual's quotidian existence, aided by pervasive computing technologies" (Allen, 2011, p. 163). The life-log can prospectively store data "[…] pertaining to biological states derived from continuous self-monitoring of, for example, heart rate, respiration, blood sugar, blood pressure, and arousal" (Allen, 2011, p. 164). The storage potential for information of a life-log can be much more extensive than the storage potential of the consciousness membrane. Because of the change from an analogue to a digital environment, it is no longer obvious that the first person LoA is the most extensive. A multi-agent system's life-log can be the third-person LoA of the system

[45] This example has partly been borrowed from Floridi (2013, p. 311).

in question. Since this LoA can contain a larger set of observables that the first-person LoA, the information propinquity of the multi-agent system can be disrupted in that external informational entities can make more detailed models of the system than the system itself. A multi-agent system's capacity for self-unification is diminished in that a larger core or nucleus set of the system in question can be unified externally to the originate system.

By self-unification, I suggest the informational person as a *self-unifying* [46] informational agent. The informational person has the capacity to *self-unification* insofar it is able to construct and sustain itself as an informational person i.e. is able to internally construct stable, coherent, models of itself from its *core* or *nucleus* set of information encapsulated within its consciousness membrane extracted from its data structures. This can only be achieved by unifying its information by means of the proper degree of encapsulation without the threat of improper or unauthorized external manipulation or alteration to the *core* or *nucleus* information of the informational person. This means that all elements of the core or nucleus set of information, encapsulated within the consciousness membrane is *prima facie* worthy of respect and protection. The onus of justification is accordingly always on those who claim or require access to the *core* or *nucleus* set of information of an informational person.

In this section, I will thus argue that the harm in taking $Mary^{C}$, is in subjecting $Mary^{i}$, to disruption of information propinquity or self-unification through improper external manipulation of her core or nucleus information. I will argue for informational integrity as the moral criterion for what information is to count as worthy of protection, and then ground the right to informational integrity or informational privacy rights on the fundamental or direct value of personal information. The direct value of personal information will then be claimed as the foundation for inferring moral principles of informational behaviour.

According to Collier any autonomous[47] system "[…] uses its own information to modify itself in order to enhance its survival […]" (2004, p. 164). According to the account of the person as a multi-agent system (consisting of a corporeal, a cognitive, and a consciousness membrane), this capacity is effectuated and optimized by the consciousness

---

[46] I have borrowed this term from Matthews (2008, p. 156), however, on my account, self-unification is not to be considered as the capacity to "[…] constructing the right kind of self narrative we regard as valuable" (Matthews, 2008, p. 156), but simply as the capacity to the right level of informational detachment or separation in order to maintain a unified set of information free from improper alterations.

[47] 'Autonomous' here meaning an ability to change state by performing internal transitions (Floridi, 2013, p. 140).

membrane's encapsulation of semantic information and informational processes such that the observed system can be the same as the system of the observer. By this, the system can make models of itself in order to optimize the interactions between its own agents so as to maintain the stability of the whole system and enhance its survival. As mentioned in Chapter 2, the historically presupposed, essential privileged self-understanding of the person must be rejected on both philosophical and scientific grounds with the realization that there is no metaphysical boundary between mind and body (Alfino and Mayes, 2003). McGeer suggests that, although the means for gaining information about oneself and others may differ, the kind of information gained in both cases is the same, the difference between a first- and third-person perspective being that of the amount in information gathered. Our first-person authority rests on our judgements of ourselves being based on a greater amount of information, or in other words, on a more detailed set of information than the judgements others make of us (McGeer, 1996, p. 500). This, however, means that we do not necessarily have privileged access to the unique (i.e. our own) information that guarantees our individuality (Alfino and Mayes, 2003).

In informational terms, first-person authority depends on there being two informational sub LoAs. The first-person LoA^i being lower than a third-person LoA^i, in that the set of observables available in the first-person LoA^i is more detailed than the available set of observables in the third-person LoA^i. This provides the systems with the capacity to make models of itself that are robust to external (and internal) informational fluctuations that might disrupt its informational integrity, and by that provide stability to the system. In pre-digital time, the person's informational unification was *naturally* sheltered from massive or invasive forces that may interrupt the system's privileged self-understanding or -unification, by the encapsulations of information within the membranes that provided it with its essential first-person LoA^i. When, however, such encapsulation, within the digital environment, is diminished, although the means for collecting and unifying information in order to construct models of oneself or others might still differ, the two sub LoA^is may converge. Analysis from the first-person LoA^is needs no longer be lower or more detailed than analysis made from the third-person LoA^i, and the multi-agent system is prone to external disruptive forces.

In line with Rössler (2005, p. 126), the EDPS (2012) considers the concerns relating to informational privacy, as the risk of de-anonymized information being distributed outside its sphere of interest to third parties who may use this information for other purposes than that what it was collected for in the first place, namely that of energy conservation. The vast

amount of data collected through smart metering allow external construction of detailed profiles or models of the person, in this case, Mary[i], in order to serve the interests of third parties. For instance, law enforcement agencies, insurance companies, tax authorities, landlords, employers etc. may all have interest in gaining information about Mary's energy consumption (EDPS, 2012).

Rössler (2005, pp. 126-127) claims that protection of informational privacy is colliding with an elementary right, namely that of looking at the world as and when one wants. Rössler sees conflicts involving protection of informational privacy as conflicts between interests in anonymity and "de-anonymization". These conflicts are thus conflicts between interests in liberty, that is, conflicts between "wanting to know" and "wanting to hide". To determine when which of these interests in liberty is to overtrump the other, the normative crux being "[…] to what extent it is acceptable for one person's profit to be at the expense of another's de-anonymization" (Rössler, 2005, p. 128). A balanced assessment must thus be made of

> [w]hat aspects of a person's life are affected by such a restriction on her informational self-determination, and, more generally, what social practices? How likely is it to result in an actual reduction in the person's freedom? How far will the individual's everyday existence (as opposed to exceptional situations) be affected? (Rössler, 2005, p. 128)

What is lacking in Rössler's (as in most) account of the right to informational privacy, is a sufficient division between types of information. Although Rössler distinguish four groups of privacy relevant information or data[48], personal information is not considered valuable as such, but only becomes worthy of protection, relative to a " […] *context* in which data protection or the protection of informational privacy acquires significance" (Rössler, 2005, p. 124, italics in the original). By this, Mary's claim to her own personal information is to be considered relative to any interested third parties and their motives for collecting and possessing the very same information. The determinative point being that of the estimated impact of external collecting and possession of information about Mary, on Mary's everyday life in relation to her established civil liberties. By, however, recognizing the impact of the "information revolution"[49] on Mary's everyday life, in that, as mentioned above, the

---

[48] See footnote 28 above for an overview of these groups.

[49] Floridi refer to the information revolution as the acceptance of the idea "[…] that we are not standalone and unique entities, but rather informationally embodied organisms […], mutually connected and embedded in an

development of new ICTs is, so to speak, changing the rules of the game, one will realize that the conflicts involved in protection of informational privacy no longer is a conflict between "wanting to know" and "wanting to hide". That is, it is not a conflict between wanting anonymity and wanting de-anonymization, but a conflict between unification and de-unification. As mentioned above, from an informational viewpoint, through smart metering of Mary's energy consumption, Mary[i], is integrated into a digital network through the patterns of organization of Mary's energy consumption, that, by the inverse function, can (due to the possibility to collect finely grained, detailed data of Mary's energy consumption) lead back to patterns of organization (information) of the core or nucleus set of information of Mary. When Mary is integrated into the digital environment, Mary's "natural" protection, i.e. encapsulation is diminished, and her control over access is more or less non-existent. Rössler says that

> The problems arising with new technologies and the associated possibilities for surveillance of course go beyond the realm of *individual* information control and extend to the sorts of *democratically delegated, state* control that people (must be able to) rely upon for the protection of their informational privacy (Rössler, 2005, p. 118, italics in the original).

These problems, however, are due to the de-encapsulation of personal information within the digital environment. If the impact of de-encapsulation is not fully recognized by accounts of informational privacy, the democratic state does not have, by the traditional liberal concepts of personal information and informational privacy, a relevant understanding of the value of personal information. By recognizing the person as information, the direct value of personal information becomes apparent, and adequate context independent principles of the rightful treatment of personal information can be adopted.

As argued in the previous chapter, on an informational account, personhood is to be conceived as the encapsulation of information of the multi-agent system i.e. person at the level of consciousness. From an informational view, this means the system is capable of self-interpretation by adapting or repurposing information and analysing herself through a first-person LoA[i], to the effect of detaching or separating herself from nature, and through this separation *the self* emerges (Floridi, 2011). The informational person is *unifying* or differentiating herself from others by encapsulating, and, by that, unifying her *core* or

---

informational environment, the infosphere, which we share with both natural and artificial agents similar to us in many respects" (Floridi, 2010c, p. 11)

nucleus information of the consciousness membrane to the effect of separating *herself-set* from the world. Due to the separation from its external environment, the "world" the system must integrate into, is a world of meanings and interpretations autonomously constructed by the "collaborative and cumulative effort by generations through time" (Floridi, 2011, p. 560). This world is thus a world of models. Although the person may be dependent on others in order to integrate herself into this world, the self emerges from its separation from nature (Floridi, 2014, pp. 92-93), keeping the information secure from unwanted or improper alterations that will disrupt the unity, and separation or detachment of the self-set is thus crucial. When the person is conceived of as constitutively made of information, any changes in her information will alter the informational person herself. A person can thus be altered either directly, by external informational agents or entities making changes in this information by copying/collecting, storing, editing, distributing etc. the information in question, or indirectly, by the informational entity adding, adapting or repurposing information received, by the informational person, from external informational entities, and by that indirectly being altered by the external informational agent or entity in question.

When Mary is integrated into the digital environment, in this case through a networked smart meter, copies of Mary's core or nucleus information can be made and freely distributed throughout the digital environment. By this, Mary as an information object has been manipulated, irrespective of who or what collected, copied, stored, or distributed her, and their motives for doing this. When information or elements of the core or nucleus set are copied, these are, strictly speaking, no longer numerically identical, to the effect of divisions being made of Mary in the digital environment, and Mary has become informationally fragmented. Any such manipulation of $Mary^{i}$, is at the risk of destabilizing $Mary^{S}$, recall that Mary as an information object is stabilized by a unification into a self of the multi-agent system, by the system, i.e. Mary, making internally coherent models of herself. Since the overall stability of the system is maintained by coherence between the system's semantic interpretations of its own system (by making the three agents of the system working together as one unit), the more extensive opportunities of external manipulation, the greater the risk of making $Mary^{i}$ incoherent.

By it being possible to conceptualize the person as a self-unifying or distributed multi-agent system of informational agents, it seems appropriate that some value should also be attached to the information itself, in order to protect the informational person from improper alterations by external informational agents. The concept of the person as

constitutively informational, gives the opportunity to make a clear *normative* distinction between two types of information. As defined at the beginning of this chapter, morally relevant information is information with direct moral relevance in relation to the informational person. Morally "irrelevant" information on the other hand is only morally relevant indirectly in relation to the person, in that information in terms of knowledge can characteristically be valued as an end by an evaluator. Informational privacy rights are justified on the direct value of personal information. More precisely, the first-person LoA^i is the person's core or nucleus set of information. This LoA^i should, due to being of direct value to the informational person (the nucleus set is the set being the set of observables through which the system construct itself, i.e. its models of itself), be considered morally relevant. First-person LoA^i, i.e. the morally relevant set of observables, indicates that the system under observation is the same as the system of the observer. Our normatively privileged LoA^i of our own system is "naturally" protected by encapsulation of the consciousness membrane in order to maintain stability. That is, the mechanism of self-unification that maintains coherence of the informational *self* is the encapsulation of information and informational processes provided by the consciousness membrane. "External" models resulting from a third-person LoA^i (i.e. set of observables) may disrupt the coherence of the originate set, and the more detailed third-person LoA^i, the greater the risk of disrupting coherence.

As argued above, the value of personal information is relevant to the multi-agent system due to the particular constitutive relation it has to its own personal information. When this relation is realized, any treatment of its constitutive information is a treatment of the multi-agent person herself. Any treatment of personal information is that of manipulation, and any manipulation of the system's personal information is a manipulation of the system itself, in that, manipulation of the personal or constitutive information of the system is a manipulation of the model which is supposed to promote its (the system's) stability. Within the digital informational environment, the multi-agent system's "natural" protection against improper manipulation is diminished or eliminated. In order to minimize the risk of informational disruption, the informational person is dependent on informational agents' obligation regarding the treatment of her constitutive or personal information. Since the informational person, constitutively, is his or her own personal information, informational obligations owed the informational person, are obligations owed the information itself. That is, as informational agents we have some direct duties regarding our treatment of personal information.

As mentioned above, what is to count as personal information is determined by the inverse function of a set. This means that informational agents[50] have duties regarding the treatment of any information that can, by the inverse function, strictly be led back to a specific/unique multi-agent system (consisting on the three membranes mentioned above). For instance, in terms of Himma,

> [a person's] right to life […] is constituted in part by certain obligatory constraints on the behavior of other moral agents; in particular, others are constrained from intentionally killing [a person] unless [she] is culpably posing a threat of death or grievous bodily harm to some other rights-holder (Himma, 2004, footnote 2, my insertions)

That is, the onus of justification is always on the killer because the act of killing is that of subjecting the system in question to an external disruptive, or rather, destructive force. Third parties' manipulation of personal information is in the same manner (at least to a certain degree) an external disruptive force taking action on the multi-agent system in question. The onus of justification of informational disruption should therefore always rest on the external manipulator. A person's right to informational privacy is thus to be established on an obligatory restriction on the informational behaviour of collecting, copying, storing and distributing elements of external core or nucleus sets of information. By this, informational privacy is provided the comprehensive protection Benn (1988) and Rössler (2005) sought after in the value of autonomy, in that informational privacy is not only to be taken into consideration due to the person's right in having its well-being taken into consideration in deliberations of external treatment of personal information. On the other hand, being grounded on the informational nature of the person, personal information is provided with a more robust protection than the theories of informational privacy rights based on the value of autonomy can provide. By being of direct moral value, personal information places, independently of context, obligatory constraints on external agents' informational behaviour.

As mentioned above, improper or unauthorized external alteration or manipulation of information protected by informational privacy rights is any collecting, copying, storing,

---

[50] Defining what informational agents are to count as moral agents is not of concern here. I do suggest, however, that as computer scientists and engineers are moral informational agents, as are all other multi-agent systems (consisting of the three membranes), those who create and construct the (digital) informational environment are under obligation to construct any artificial informational agents and patterns of interaction in the informational environment in consistency with obligations to informational behaviour, as well as every multi-agent system having their personal "informational" duties.

distributing, and editing of this information, since such activities can disrupt the unity of the set. Floridi states that informational privacy is to be considered as the fundamental and inalienable right to

> […] immunity from unknown, undesired, or unintentional changes in one's own identity as an informational entity both *actively* and *passively*. Actively, because collecting, storing, reproducing, manipulating, etc. one's information amounts now to two stages in stealing, cloning or breeding someone else's personal identity. Passively, because breaching one's informational privacy may now consist in forcing someone to acquire unwanted data, thus altering her or his nature as an informational entity without consent (Floridi, 2013, pp. 243-244).

Similarly, I have suggested a definition of the right to informational privacy as the fundamental right to informational integrity. Since this set is what constitutes the self, the unity of this set is worthy of protection insofar as it sustains the informational agent in question, that is, the multi-agent system. Informational privacy is, then, understood as the state of *self-unification*, that is, as the state of being a unified set of information by enjoying the right degree of separation or detachment from the world. As mentioned in the previous chapter, the capacity for storing information in the original set is limited. This gives rise to the possibility, by the unlimited capacity of external informational entities for storing information, of copied self-sets being larger than itself. When distribution also is unlimited, the unauthorized copy can then be distributed, not only to other regions of the informational environment, but back to the original set, and by that unauthorized parts are added to the original set in question. This will infringe upon the set's self-unification, by implementing disorder and inconsistency into the system in question, both by making unique information non-unique by copying (and distributing) it to other regions of the "world," and by that decreasing its detachment or separateness from the world. The set's self-unification can also be reduced by the ability to distribute back to the original set, either deleted information or information the originator would like to have deleted, making the set inconsistent with itself, and by that forcing unwanted alterations upon the set in question.

When the self emerges from informational separateness or disconnectedness, the capacity to separate/disconnect or detach information from the world is a precondition for autonomy, since, without it, there would be no selves or personhoods, neither in form of autonomy or any other valued human attribute. Informational privacy is thus not valuable because we are autonomous, or because of any other valued human attribute, but these human attributes are possible because we are "informationally" detached or separated/disconnected

from the external environment, i.e. because we have informational privacy. Without informational privacy or informational detachment we cannot be a unity of information. When the external environment becomes a digital informational environment, the detachment or unity of our selves as sets of information, is not obvious. By this, informational privacy rights are the protection of the unity of the informational person. That is, the right to informational privacy is the right to informational integrity of the *core* or *nucleus* information, encapsulated in the consciousness membrane; together with the right to informational integrity of the *core* or *nucleus* information encapsulated within the corporeal and cognitive membrane that can, by improper external manipulations and distribution, disrupt the unity of the *self-set.* Instead of making a normative distinction between the "natural"[51] person and her information, to the effect of having to take a roundabout way of ascribing moral value to personal information via the former, it seems proper to ground informational privacy rights on a concept of the person that can provide a direct value of personal information when such a conception is available.

4.5 Some Objections to Basing Informational Privacy Rights on the Informational Person

An objection against the informational re-conceptualization of personhood that could be raised by Benn and Rössler is, that by changing the premise of personhood one is deflating the subject in that the person is no longer primarily a conscious autonomous mind but a system, to the effect of not providing a clear conception of the informational right holder. The problem being, that treating persons purely as computational systems, the person will become a purely formal notion. That is, "[…] where one draws the line around the physical region that is being represented computationally is left entirely to the discretion of whoever is constructing the computational representation" (Millgram, n.d.). An informational conception of personhood where the person is equated with a set of information and informational processes, i.e. an informational system, does not provide for a clear-cut definition of what is to count as 'the person' in that the person can be extended to include anything or indeed everything. In other words if the person is a self-unifying set of information there is nothing

[51] 'Natural' here meaning autonomous as in terms of Benn (1988) or Rössler (2005).

stopping the person from including more or less random objects, such as a piece of land, as part of her system. Nucleus information of the land is thus to be considered as personal information of the new system and this information, as "personal" information, has a claim on others to treat it in accordance with obligatory informational behaviour. In my opinion, however, this objection arises from not recognizing the particular type of system the person is considered as. Zang, et al. distinguish between three kinds of systems: centralized systems, where the components of the system are restricted to one site; decentralized systems, where the components of the system are at different sites with no or limited coordination; and, distributed systems, where the components of the system are relatively autonomous entities but work together to achieve some overall objective (Zang, et al., 2004). The person as a multi-agent system is, as argued in Chapter 3, to be considered a distributed system, the overall objective of the system being that of maintaining stability of the system as a whole. If the person as a multi-agent system is to be extended to include additional, externally encapsulated, sets of information and informational processes than those included in the originate system; such external informational objects must satisfy the condition of coordination required for a distributed system. That is, if the person or multi-agent system is to be successfully extended to include, for instance, a piece of land, the piece of land must be working together with the other agents included in the system, sharing processing powers with them, and the originate agents included in the person as multi-agent system together with the piece of land in question must appear as a unity. Informational objects or agents included in the multi-agent system can thus only extend to those agents that can show a homeostatic function or contribution in relation to the whole system of which it is claimed to be a part. This, however, still leaves the informational conception of personhood flexible enough to extend the person or multi-agent system to external informational processing units such as smart devices etc. and so moral status could be extended to such devices, turning the devices in question into right holders of informational privacy rights.

On the other hand, it could be argued that allowing for the person being extended to external devices does not preserve the autonomy of the self, and that such external extension comes with the cost of leaving informational privacy rights unjustified. If external informational devices, equipped with better informational processing abilities than the original system, could be developed, it will be in the system's interest to allow unlimited distribution and access of personal information in order to outsource information processing to such external processing devices. The stability of the system could be maintained more

sufficiently by having one's personal information processed by external units or parties, to the effect of stripping the notion of autonomy of value. Extensive distribution of personal information is, however, in itself a de-stabling factor of the system. As mentioned in section 4.2, the system is dependent upon optimizing its (behavioural) unity in order to maintain its stability. It is due to its (behavioural) unity that the system is able to resist disruptive forces. Such unity, however, is achieved through its degree of separation from the external environment. Collier states autonomy or independence as a special type of unity relation, "[i]ts distinguishing feature is that cohesion is maintained actively through the contributions of component processes to the continued existence of the system, either directly, or through intermediate processes" (Collier, 2002). The person i.e. multi-agent system's degree of informational detachment from the world results in the unity of the system being maintained by the system's self-modelling activity, that is, by the system actively creating its own *self*-models. Extensive external interference to this activity jeopardizes the system's self-modelling abilities, in that such intrusion diminishes its internal unity relations with its parts. One could, for example, imagine that a system's (i.e. person's) body could be networked with external information processing units, in order for the external unit to replace activity originally undertaken by the shared effort of the (original) system. For instance, sensors detecting hunger could be placed within the system, sending information of the system's energy state to an external unit, in order for the external unit to take appropriate action to satisfy the needs the system has relating to this state. The system would no longer depend on making a "hungry-model" of itself in order to satisfy its hunger, since this analysis would be made externally to the system. The system's unity relation of its agents would be diminished in that the system's agents need not work together in order to achieve the behavioural unity normally required for eating. The system becomes de-unified and needs no longer appear (to itself) as a unity in order to relieve its hunger, and the system, as a distributed system, is no longer sustained[52]. The multi-agent system is thus more stable by not being extensively interfered with by external forces, and the informational re-conceptualization of personhood is not incompatible with the value of autonomy, since preserving the system's (behavioural) unity is (in at least some meaning of the word) due to the system being autonomous.

I acknowledge that an informational re-conceptualization of personhood may seem

[52] This could be remedied by extending the system to include external information processing units, however, to the effect of forfeiting the informational integrity of the system. Extending the system to external information processing, by allowing extensive distribution of personal information, could leave the multi-agent system informationally fragmented, to the effect of there being nothing or little left of the original system.

rather counter-intuitive to many, and, that informational privacy rights based on the direct value of personal information, can make informational privacy rights seem controversially comprehensive. I nevertheless believe the informational re-conceptualization of personhood as the foundation of informational privacy rights to be appropriate (at least to be taken into consideration), in view of the fast and controversial changes made to our lives by the development in Information and Communication Technologies. In order to handle the radical changes these technologies make on our "world" and our place in it, we need informational privacy rights that are based on a conception of personhood that accommodates these changes.

5 Conclusion

In this thesis, I have argued against the liberal accounts of Benn and Rössler, basing informational privacy rights on the conception of personhood in terms of autonomy. I have argued that the value of autonomy is not capable of securing our needs to informational privacy within the digital informational environment, since informational privacy rights based on the value of autonomy only provide us with control rights, that is, with rights to control others' access to our own personal information in certain situations, and thus are not capable of formulating moral standards for how personal information is to be treated within a digital informational environment. Control rights are not sufficient in protecting individuals' informational privacy rights within an environment that does not accommodate individuals' ability to control their own information flow. As we find ourselves increasingly partaking in a digital informational environment – in which both persons (like any other entity inhabiting this environment) and their patterns of interaction (i.e. information flow) are created by computer engineers – when seeking to formulate relevant or appropriate rights to right holders, we should use a concept of the right holder and her abilities that matches the nature and the abilities of the right holder within the environment she is holding these rights in.

Discussion of informational privacy is frequently induced by concerns relating to improper manipulation of personal information within the digital informational environment. In this environment any entity (including persons, i.e. individual rights holders) is nothing other than (sets of) data or information that can be unrestrictedly operated on by information processing powers. An account of informational privacy rights, based on a concept of personhood in terms of autonomy, presupposes personal information as something separate from the person in question. By this, any moral status granted the person is not extended to her information, and any constraints on external access to personal information must be justified by turning to how and in which contexts such access infringes upon the person's possibilities for living autonomously, personal information as such being without any moral value. By these theories, the moral value of the (informational) person within the digital informational environment becomes unclear, since, within the informational environment, a person is personal information. This is problematic in view of the fact that our living increasingly is taking place, and is expected by others to be taking place, within this environment. Within the digital informational environment, to provide adequate protection of the person's informational privacy or integrity, a conception of the person as a set of information of a particular kind (i.e. as a set of morally relevant information) is needed in

order to justify moral constraints on behaviour towards personal information.

In this thesis I have claimed that such a conception is available through Floridi's (2011) account of the informational person. I have suggested that, on this account, the person can be conceptualized in terms of a self-modelling multi-agent system, maintained by the agents' capacity to encapsulate or unify information to the effect of preserving the agent's or system's stability. I have argued that the self-modelling multi-agent system is optimizing its overall stability by being self-unifying in its model-making, that is, the system is constructing its *self*-models by observing and interpreting its own data-structures (and information) to the effect of ending up with a model of itself. The moral value of personal information is the value, in relation to a self-modelling multi-agent system, in being constitutive of its models (i.e. its *self*). Since, however, the system does not have direct access to its own data-structures, there can be many and various and equally appropriate interpretations of the same system, both by internal and external analysis to the effect of a multitude of various models. The informational person being the sum of all appropriate models of its system. Thus, by collecting someone's personal information one is at the same time adding to the sum of models and by that also altering the informational person in question, this person running the risk of a de-stabilizing informational fragmentation. By this, when collecting or manipulating elements of a set of personal information, one is at the same time altering the informational person in question. Thus, by treating personal information one is treating the person herself, and personal information is entitled the moral commitment or respect of others. By realizing that the person can be conceptualized in terms of information, the direct value of personal information is recognized and the "real" harm in violations of informational privacy can be articulated as improper manipulations of the informational person herself. By this, informational privacy rights in form of obligatory constraint on behaviour towards personal information can be established.

The aim of this thesis has been to suggest or promote a moral foundation for informational privacy rights that reflects challenges to informational privacy of the individual, materialized through developments in Information and Communication Technologies. I have concluded that rights to informational privacy that provide sufficient protection to the individual is achieved only by an account of informational privacy rights that recognizes the informational nature of the person, and thus ascribes moral status to personal information, through which moral duties towards personal information can be defined or developed. I have not, however, given a definition of what obligations such duties

might involve. Defining both informational duties, or obligations, we might have towards our own personal information, and informational duties we owe others, must, then, be the task of future work.

While recognizing and appreciating the extensive and controversial moral, legislative, and political implications implicit in grounding informational privacy rights on an informational conception of personhood; in my view, considering the extensive (and controversial) implications of the information revolution to our lives, we must, just as we embrace technological advances, also be open to conceptual developments – even if such developments may affect other established liberties – in order to be equipped to deal with the challenges thrown at us when living in a radically technologically advanced world.

Reference List

Al-Fedaghi, S. S. (2005) "How to Calculate the Information Privacy". *Proceedings of the Third Annual Conference on Privacy, Security and Trust (PST 2005)* [online], October 2005, St Andrews, New Brunswick. Available at: <http://pdf.aminer.org/000/554/759/how_to_calculate_the_information_privacy.pdf> [Accessed 22.03.2013].

Al-Fedaghi, S. S. (2006) "The 'Right to be Let Alone' and Private Information". In: Chen, C. -S., Filipe, J., Secura, I. and Cordeiro, J. (eds.), *Enterprise Information Systems VII* [e-book], pp. 157-166. Dordrecht: Springer. Available from: <http://link.springer.com/book/10.1007/978-1-4020-5347-4> .

Alfino, M. and Mayes, G. R. (2003) "Reconstructing the Right to Privacy". *Social Theory & Practice* [online], 29 (1), pp. 1-18. Available through: <http://philpapers.org/rec/ALFRTR> [Accessed 03.08.2013].

Allen, A. L. (2011) *Unpopular Privacy: What Must We Hide?* New York: Oxford University Press.

Bates, M. J. (2005) "Information and Knowledge: An Evolutionary Framework for Information Science". *Information Research* [online], 10 (4). Available at: <http://www.informationr.net/ir/10-4/paper239.html> [Accessed 22.01.2014].

Bates, M. J. (2006) "Fundamental Forms of Information". *Journal of the American Society for Information Science and Technology* [online], 57 (8), pp. 1033-1045. Available from: <http://dx.doi.org/10.1002/asi.20369> [Accessed 20.01.2014].

Bawden, D. (2007) "Organized Complexity, Meaning and Understanding: An Approach to a Unified View of Information for Information Science". *Aslib Proceedings* [online], 59 (4-5), pp. 307-327. Available from: <http://dx.doi.org/10.1108/00012530710817546> [Accessed 20.01.2014].

Benn, S. I. (1984) "Privacy, Freedom, and Respect for Persons". In: Schoeman, F. D. (ed.), *Philosophical Dimensions of Privacy: An Anthology,* Cambridge: Cambridge University Press. pp. 223-244.

Benn, S. I. (1988) *A Theory of Freedom,* Cambridge: Cambridge University Press.

Brazier, F. Oskamp, A., Prins, C., Schellekens, M., and Wijngaards, N. (2004) ”Law-abiding and integrity on the Internet: A case for agents”. *Artificial Intelligence and Law* [online], 12 (1-2). pp. 5–37. Available from: <http://dx.doi.org/10.1007/s10506-004-6250-z> [Accessed 21.12.2014].

Bynum, T. W. (2008) “Norbert Wiener and the Rise of Information Ethics”. In: Van den Hoven, J. and Weckert, J. (eds.), *Information Technology and Moral Philosophy* [e-book], Cambridge: Cambridge University Press. pp. 8-25. Available from: <http://dx.doi.org/10.17/CBO9780511498725> .

Bynum, T. W. (2010) “Philosophy in the Information Age”. In: Allo, P. (ed.), *Putting Information First: Luciano Floridi and the Philosophy of Information,* Chichester: Wiley-Blackwell. pp. 171-193.

Ciancarini, P and Wooldridge, M. J. (2002) “Agent-Oriented Software Engineering: The state of the Art”. In: Ciancarini, p. and Woolridge, M. J. (eds.), *Agent-Oriented Software Engineering: First International Workshop, AOSE 2000 Limerick, Ireland, June 10, 2000 Revised Papers* [e-book], Berlin: Springer, pp. 1-28. Available through: <http://link.springer.com> .

Colburn, T. and Shute, G. (2010) “Abstraction, Law, and Freedom in Computer Science”, in: Allo, P. (ed.), *Putting Information First: Luciano Floridi and the Philosophy of Information,* Chichester: Wiley-Blackwell. pp. 97-115.

Colburn, T. and Shute, G. (2011) “Decoupling as a Fundamental Value of Computer Science”. *Minds and Machines* [online], 21 (2), pp. 241-259. Available from: <http://dx.doi.org/10.1007/s11023-011-9233-3> [Accessed 18.11.2013].

Collier, J. (2002) *What is Autonomy?* [online], Available through: <http://philpapers.org/rec/COLWIA> [Accessed 10.02.2014].

Collier, J. (2004) “Self-Organization, Individuation and Identity”. *Revue internationale de philosophie* [online], 2 (228), pp. 151-172. Available from: <http://www.cairn.info/revue-internationale-de-philosophie-2004-2-page-151.htm> [Accessed 10.02.2014].

Conti, M., Das, S. K., Bisdikian, C., Kumar, M., Ni, L. M., Passarella, A., Roussos, G., Tröster, G., Tsudik, G., and Zambonelli, F. (2012) “Looking Ahead in Pervasive Computing: Challenges and Opportunities in the Era of Cyber-Physical Convergence”. *Pervasive and Mobile Computing* [online], 8 (1), pp. 2-21. Available from: <http://dx.doi.org/10.1016/j.pmcj.2011.10.001> [Accessed 03.04.2014].

Dennett, D. C. (1992) “The Self as a Center of Narrative Gravity”. In: Kessel, F., Cole, p., and Johnson, D. (eds.), *Self and Consciousness: Multiple Perspectives* [online Book Chapter], Hillsdale, NJ: Erlbaum. Available through: <http://cogprints.org/266/> [Accessed 15.01.2014].

Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., and Maisel, W. H. (2010) “Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices”. *CHI’10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* [online], April 10-15, Atlanta, Georgia. Pp. 917-926. Available at: <http://dl.acm.org/citation.cfm?doid=1753326.1753462> [Accessed 04.04.2014].

European Data Protection Supervisor, (2012) *Opinion of the European Data Protection Supervisor: On the Commission Recommendation on Preparations for the Roll-out of Smart Metering Systems* [online], Available at: <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf> [Accessed 04.02.2014].

Fletcher, R. R., Dobson, K., Goodwin, M. S., Eydgahi, H., Wilder-Smith, O., Fernholz, D., Kuboyama, Y., Hedman, E. B., Ming-Zher Poh,, and Picard, R. W. (2010) “iCalm: Wearable Sensor and Network Architecture for Wirelessly Communication and Logging Automatic Activity”. *Information Technology in Biomedicine, IEEE Transactions on* [online], 14 (2), pp. 215-223. Available from: <http://dx.doi.org/10.1109/TITB.2009.2038692> [Accessed 15.03.2014].

Floridi, L. (1999) “Information ethics: On the philosophical foundation of computer ethics”. *Ethics and Information Technology* [online], 1 (1), pp. 37-56. Available from: <http://dx.doi.org/10.1023/A:1010018611096> [Accessed 30.06.2013].

Floridi, L. (2002) “On the intrinsic value of information objects and the infosphere”. *Ethics and Information Technology,* [online], 4 (4), pp. 287-304. Available from: <http://dx.doi.org/10.1023/A:1021342422699> [Accessed 18.09.2013].

Floridi, L. (2005) “The ontological interpretation of informational privacy”. *Ethics and Information Technology* [online], 7 (4), pp. 185-200. Available from: <http://dx.doi.org/10.1007/s10676-006-0001-7> [Accessed 29.06.2013].

Floridi, L. (2010a) *Information: A Very Short Introduction*, Oxford: Oxford University Press.

Floridi, L. (2010b) “The Philosophy of Information as a Conceptual Framework”. *Knowledge, Technology & Policy* [online], 23 (1-2), pp. 253-281. Available from: <http://dx.doi.org/10.1007/s12130-010-9112-x> [Accessed 13.01.2014].

Floridi, L. (2010c) “Ethics after the Information Revolution”. In: Floridi, L. (ed.), *The Cambridge Handbook of Information and Computer Ethics,* Cambridge: Cambridge University Press. pp. 3-19.

Floridi, L. (2011) “The Informational Nature of Personal Identity”. *Minds and Machines* [online], 21 (4), pp. 549-566. Available from: <http://dx.doi.org/10.1007/s11023-011-9259-6> [Accessed 10.09.2013].

Floridi, L. (2013) *The Ethics of Information,* Oxford: Oxford University Press.

Floridi, L. (2014) “Perception and Testimony as Data Providers”. In: Ibekwe-SanJuan, F. and Dousa, T. M. (eds.), *Theories of Information, Communication and Knowledge: A Multidisciplinary Approach* [e-book]*,* Studies in History and Philosophy of Science 34, London: Springer. pp. 71-95. Available from: <http://link.springer.com/book/10.1007/978-94-007-6973-1> .

Grice, H. P. (2010) “Meaning”. In: Martinich, A. P. (ed.), *The Philosophy of Language.* 5th int. ed. New York: Oxford University Press. pp. 108-113.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013) “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions”. *Future Generation Computer Systems* [online], 29 (7), pp. 1645-1660. Available from: <http://dx.doi.org/10.1016/j.future.2013.01.010> [Accessed 08.03.2014].

Hernandez, J., McDuff, D., Fletcher, R., and Picard, R. W. (2013) “Inside-Out: Reflectin on your Inner State”. *Pervasive Computing and Communications Workshops (PERCOM Workshops) 2013, IEEE International Conference on* [online], March 18-22, San Diego, CA. Available from: <http://dx.doi.org/10.1109/PerComW.2013.6529507> [Accessed 15.03.2014].

Himma, K. E. (2004) “There’s Something About Mary: The Moral Value of Things Qua Information Objects”. *Ethics and Information Technology* [online], 6 (3), pp. 145-159. Available from: <http://dx.doi.org/10.1007/s10676-004-3804-4> [Accessed 05.01.2014].

Hongladarom, S. (2011) “Pervasive Computing, Privacy and Distribution of the Self”. *Information* [online], 2 (2), pp. 360-371. Available from: <http://dx.doi.org/10.3390/info2020360> [Accessed 20.09.2013].

Hongladarom, S. (2013) “Ubiquitous Computing, Empathy and the Self”. *AI & Society* [online], 28 (2), pp. 227-236. Available from: <http://dx.doi.org/10.1007/s00146-012-0395-1> [Accessed 15.09.2013].

Howard, D. M. and Angus, J. (1996) *Acoustics and Psychoacoustics,* Oxford: Focal Press.

Hrbacek, K. and Jech, T. (1999) *Introduction to Set Theory,* 3rd ed. Boca Raton, FL: CRC Press.

Korsgaard, C. M. (1996) *Creating the Kingdom of Ends,* Cambridge: Cambridge University Press.

Korzenny, F. (1978) “A theory of Electronic Propinquity: Mediated Communication in Organizations”. *Communication Research* [online], 5 (3), pp. 3-24. Available from: <http://dx.doi.org/10.1177/009365027800500101> [Accessed 22.02.2014].

Lieberman, M. D. (2012) “Self-Knowledge: From Philosophy to Neuroscience to Psychology”. In: Vazire, S. and Wilson, T. D. (eds.), *Handbook of Self-Knowledge,* New York: The Guilford Press. pp. 63-76.

Lisovich, M. A. and Wicker, S. B. (2008) “Privacy Concerns in Upcoming Residental and Commercial Demand-Response Systems”. *IEEE Proceedings on Power Systems* [online], 1 (1). Available from: <https://www.truststc.org/pubs/332/lisovich2007pci_v3.pdf> [Accessed 05.02.2014].

Manders-Huits, N. (2010) “Practical versus Moral Identities in Identity Management”. *Ethics and Information Technology* [online], 12 (1), pp. 43-55. Available from: <http://dx.doi.org/10.1007/s10676-010-9216-8> [Accessed 22.07.2013].

Matthews, S. (2008) “Identity and Information Technology”. In: Van den Hoven, J. and Weckert, J. (eds.), *Information Technology and Moral Philosophy* [e-book], Cambridge: Cambridge University Press. pp. 142-160. Available from: <http://dx.doi.org/10.1017/CBO9780511498725> .

McGeer, V. (1996) “Is ‘Self-Knowledge’ An Empitical Problem? Renegotiating the Space of Philosophical Explanation”. *The Journal of Philosophy* [online], 93 (10), pp. 483-515. Available through: <http://www.jstor.org/stable/2940837> [Accessed 29.07.2013].

Millgram. E. (n.d. Work in Progress) *Private Persons and Minimal Persons* [online], Available from: <http://www.elijahmillgram.net/work-in-progress.html> [Accessed, 05.08.2013].

Moore, A. D. (2010) *Privacy Rights: Moral and Legal Foundations,* University Park: The Pennsylvania State University Press.

Roux, B. and Falgoust, M. (2013) “Information Ethics in the Context of Smart Devices”. *Ethics and Information Technology* [online], 15 (3), pp. 183-194. Available from: <http://dx.doi.org/10.1007/s10676-013-9320-7> [Accessed 30.07.2013].

Rössler, B. (2005) *The Value of Privacy.* Translated from German by Glasgow, R. D. V. Cambridge: Polity Press.

Ryle, G. (1984) *The Concept of Mind,* University of Chicago Press ed. Chicago: The University of Chicago Press.

Schoeman, F. D. (1984) “Privacy: Philosophical Dimensions of the Litterature”. In: Schoeman, F. D. (ed.), *Philosophical Dimensions of Privacy: An Anthology,* Cambridge: Cambridge University Press. pp. 1-33.

Schoeman, F. D. (1992), *Privacy and Social Freedom,* Cambridge: Cambridge University Press.

Solove, D. J. (2004) *The digital person: Technology and Privacy in the Informaton Age,* New York: New York University Press.

Solove, D. J. (2009) *Understanding Privacy,* First Harvard University Press paperback ed. Cambridge, Mass: Harvard University Press.

Vakarelov, O. (2010) “Pre-cognitive Semantic Information”. *Knowledge, Technology & Policy* [online], 23 (1-2), pp. 193-226. Available from: <http://dx.doi.org/10.1007/s12130-010-9109-5> [Accessed 13.01.2014].

Van den Hoven, J. (2008) “Information Technology, Privacy, and the Protection of Personal Data”. In: Van den Hoven, J. and Weckert, J. (eds.), *Information Technology and Moral Philosophy* [e-book], Cambridge: Cambridge University Press. pp. 301-321. Available from: <http://dx.doi.org/10.1017/CBO9780511498725> .

Warren, S. D. and Brandeis, L. D. (1984) “The Right to Privacy: The Implicit Made Explicit”. In: Schoeman, F. D. (ed.), *Philosophical Dimensions of Privacy: An Anthology,* Cambridge: Cambridge University Press. pp. 75-103.

Wasserstrom, R. A. (1984) “Privacy: Some Arguments and Assumptions”. In: Schoeman, F. D. (ed.), *Philosophical Dimensions of Privacy: An Anthology,* Cambridge: Cambridge University Press. pp. 317-332.

Wiegel, V., Van den Hoven, M. J., and Lokhorst, G. J. C. (2005) "Privacy, Deontic Epistemic Action Logic and Software Agents". *Ethics and Information Technology* [online], 7 (4), pp. 251-264.
Available from: <http://dx.doi.org/10.1007/s10676-006-0011-5> [Accessed 15.12.2013].

Woods, H. A. and Wilson, J. K. (2013) "An Information Hypothesis for the Evolution of Homeostasis". *Trends in Ecology and Evolution* [online], 28 (5), pp. 283-289.
Available from:
<http://www.sciencedirect.com/science/article/pii/S0169534712002947> [Accessed 12.09.2013].

Zhang, Z., McCalley, J. D., Vishwanathan, V., and Honavar, V. (2004) "Multiagent System Solutions for Distributed Computing, Communications, and Data Integration Needs in the Power Industry". *Proceedings of the General Meeting of the IEEE Power Engineering Society* [online], June 6-10 2004, Denver, Colorado. Available from:
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1372750 &isnumber=30010> [Accessed 30.09.2013].