Four challenges for a theory of informational privacy

Luciano Floridi[1,2,3]
[1]*Dipartimento di Scienze Filosofiche, Università degli Studi di Bari, Italy*
[2]*Faculty of Philosophy, University of Oxford, Oxford, UK*
[3]*Information Ethics Group, OUCL, University of Oxford, Oxford, UK*
E-mail: luciano.floridi@philosophy.oxford.ac.uk

Abstract. In this article, I summarise the ontological theory of informational privacy (an approach based on information ethics) and then discuss four types of interesting challenges confronting any theory of informational privacy: (1) parochial ontologies and non-Western approaches to informational privacy; (2) individualism and the anthropology of informational privacy; (3) the scope and limits of informational privacy; and (4) public, passive and active informational privacy. I argue that the ontological theory of informational privacy can cope with such challenges fairly successfully. In the conclusion, I discuss some of the work that lies ahead.

Key words: information ethics, informational privacy, ontology, passive privacy, personal identity, public privacy

Introduction

In an article recently published in this journal,[1] I outlined an ontological theory of informational privacy based on information ethics.[2] Owing to its scope and contents, four challenges, though admittedly rather important, could not be properly analysed in that proposal. They are now the subject of the following pages.

The article is divided into two parts. In the first, I provide a brief summary of the ontological approach to informational privacy. I hope this will make the perspective adopted in the rest of the article sufficiently explicit, while providing the reader with the necessary background to assess how the approach fares with respect to the challenges discussed in the subsequent sections. Although the summary is meant to make the discussion self-sufficient, the reader interested in a more detailed analysis of the ontological theory of informational privacy, and especially in the reasons offered to buttress it, may wish to consult the aforementioned article.

In the second part, I discuss four types of interesting challenges confronting any theory of informational privacy. The main point addressed there is that some problems should be taken seriously, lest our interpretation of informational privacy becomes a mere linguistic stipulation regarding the correct usage of ''privacy'' in various languages or cultural contexts. I try to show that the ontological approach can cope with such challenges fairly successfully, but I won't anticipate more, as all this will become clearer in due course.

In the conclusion, I briefly comment on some of the work that lies ahead.

The ontological interpretation of informational privacy[3]

Imagine a model of a limited (region of the) infosphere, represented by patients (our interactive, informational agents[4]) admitted to the same hospital (our limited environment).[5] Intuitively, given a

[1] L. Floridi. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, 7(4): 185–200, 2005.

[2] L. Floridi. Information Ethics. In Jeroen van den Hoven and John Weckert, editors. *Moral Philosophy and Information Technology*. Cambridge University Press, Cambridge, forthcoming.

[3] This section is a slightly revised summary of L. Floridi, The Ontological Interpretation of Informational Privacy.

[4] ''Agent'' has a variety of meanings. In other papers, I use it to refer to *interactive*, *autonomous* and *adaptable systems* that can perform *morally qualifiable actions*. This is a minimalist definition, as shown in L. Floridi and J. W. Sanders. On the Morality of Artificial Agents. *Minds and Machines*, 14(3): 349–379, 2004.

[5] For an empirical assessment see E. Bäck and K. Wikblad. Privacy in Hospital. *Journal of Advanced Nursing*, 27(5): 940–945, 1998.

certain amount of available information, the larger the *informational gap* among the agents, the less they know about each other, the more private their lives can be.

The informational gap is a function of the degree of *accessibility* of personal data. In the example, there will be more or less informational privacy depending on whether rooms in the ward are designed for one or two patients and whether each is equipped with its own bathroom.

Accessibility, in its turn, is an epistemic factor that depends on the *ontological features* of the infosphere, i.e., on the nature of the specific agents, of the specific environment in which they are embedded and of the specific interactions implementable in that environment by those agents. If the partitions in the ward are few and thin and all the patients have excellent hearing, the degree of accessibility is increased, the informational gap is reduced and informational privacy is more difficult to obtain and less easy to protect. Thus, the ontological features of the infosphere determine a specific degree of *ontological friction*, which in turn determines the information flow within the system.

Ontological friction refers here to the forces that oppose the information flow within (a region of) the infosphere, and hence (as a coefficient) to the amount of work and efforts required for a certain kind of agent to obtain, filter and/or block information (also, but not only) about other agents in a given environment, e.g., by establishing and maintaining channels of communication and by overcoming obstacles in the flow of information such as distance, noise, lack of resources (especially time, memory space and processing capacities), amount and complexity of the data to be processed, and so forth.

Of course, the informational affordances[6] and constraints provided by an environment are such only in relation to agents with specific informational capacities. In our model, brick walls afford much higher ontological friction for the flow of acoustic information than a paper-thin partition, but this is irrelevant if the patients are deaf.

To summarise: given a certain amount of personal information available in (a region of) the infosphere I, the lower the ontological friction in I, the higher the accessibility of personal information about the agents embedded in I, the smaller the informational gap among them, and the lower the level of informational privacy implementable about each of them. Put simply, *informational privacy is a function of the ontological friction in the infosphere*. It follows that any factor affecting the latter will also affect the former.

The factors in question can vary and may concern more or less temporary or reversible changes in the environment or in the agents. Because of their ''data superconductivity'', ICTs are well-known for being among the most influential factors that affect the ontological friction in the infosphere.[7] A crucial difference between old and new ICTs is *how* they affect it.

Old or pre-digital ICTs have always tended to *reduce* the ontological friction and hence informational privacy in the infosphere because they *enhance* or *augment* the agents embedded in it.

New or digital ICTs are different in that, being interactive, they can also increase informational privacy or indeed change (what one appreciates as) informational privacy insofar as they *re-ontologize*[8] the very nature of the infosphere, that is, of the environment itself, of the agents embedded in it and of their interactions. Digital ICTs are *ontologizing devices* because they engineer new environments that the user/agent is then enabled to inhabit. Let me illustrate this point with two examples.

To begin with, imagine that all the walls and the furniture in the ward are transformed into perfectly transparent glass. Assuming our patients have good sight, this will drastically reduce the ontological friction in the system. Imagine next that the patients are transformed into proficient mind-readers and telepathists. Any informational privacy in this sort of Bentham's *PanOpticon* will become virtually impossible.

As a second example, in ''The Dead Past'' Asimov describes a *chronoscope*, a device that allows direct observation of past events.[9] The chronoscope turns out to be of only limited use for archaeologists, since it can look only a couple of centuries in the past. However, people soon discover that it can easily be tuned to the most recent past, with a time lag of fractions of seconds. Through the chronoscope, one can observe any event almost in real time. It is the end of privacy, for the dead past is only a synonym for ''the living present'', as one of the characters remarks rather philosophically.

Again, these thought experiments illustrate how radical modifications in the very nature (a re-ontologization) of the infosphere can dramatically change the conditions of possibility of informational

[6] J.J. Gibson. *The Ecological Approach to Visual Perception*. Houghton Mifflin, Boston, London, 1979.

[7] For a similar point see J.H. Moor. Towards a Theory of Privacy in the Information Age. *ACM SIGCAS Computers and Society*, 27: 27–32, 1997: ''When information is computerised, it is *greased* to slide easily and quickly to many ports of call'' (p. 27).

[8] The neologism is constructed following the word ''re-engineering'' (''to design and construct anew'').

[9] I. Asimov. The Dead Past. In *Astounding Science Fiction*, 6–46, 1956.

privacy. To summarise: we saw that informational privacy is a function of the ontological friction in the infosphere. Many factors can affect such ontological friction, including, most importantly, *technological innovations* and *social developments*, such as, for example, massive inurbation (i.e., the abandonment of rural areas in favour of metropolis) and the corresponding phenomenon of anonymity. Old ICTs affected the ontological friction in the infosphere mainly by enhancing or augmenting the agents embedded into it. Therefore, they tended to decrease the degree of informational privacy possible within the infosphere. By contrast, digital ICTs affect the ontological friction in the infosphere both by allowing forms of protection of informational privacy and, most significantly, by re-ontologizing it. Not only can they both decrease and protect informational privacy but, most importantly, they can also alter its nature and hence our understanding and appreciation of it.

Interpreting the revolutionary nature of digital ICTs in this ontological way provides a fruitful approach to develop a robust theory of informational privacy. In the same way as the digital revolution is best understood as a fundamental re-ontologization of the infosphere, informational privacy requires an equally radical re-interpretation, one that takes into account the essentially informational nature of human beings and of their operations as social agents. Such re-interpretation is achieved by considering each individual as constituted by his or her information, and hence by understanding a breach of one's informational privacy as a form of aggression towards one's *personal identity*.

This interpretation is consistent with the fact that digital ICTs can both erode and reinforce informational privacy, and hence that a positive effort needs to be made in order to support not only PET (Privacy Enhancing Technologies) but also *poietic* (i.e., constructive) applications, which may allow users to design, shape and maintain their identities as informational agents.[10] The information flow requires some friction in order to keep firm the distinction between the multiagent system (the society) and the identity of the agents (the individuals) constituting it. Any society in which no informational privacy is possible is one in which no personal identity can be maintained and hence no welfare can be achieved, social welfare being only the sum of the individuals' involved. The total ''transparency'' of the infosphere – recall the example of the glassy hospital and of our mentally super-enhanced patients, or Asimov's *chronoscope* – that may be advocated by some as something to strive for, achieves the protection of society only by erasing all personal identity and individuality, a ''final solution'' for sure, but hardly one that the individuals themselves, constituting the society so protected, would be happy to embrace freely and permanently. As Cohen has rightly remarked, ''the condition of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it''.[11]

Looking at the nature of a person as being constituted by that person's information allows one to understand the right to informational privacy as a right to personal 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 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.[12] Brain-washing is as much a privacy breach as mind-reading.

The ontological interpretation suggests that one's informational sphere and one's personal identity are co-referential, or two sides of the same coin. ''You are your information'', so anything done to your information is done to you, not to your belongings. It follows that the right to informational privacy (both in the active and in the passive sense just seen) shields one's personal identity.[13] This is why informational privacy is extremely valuable and ought to be respected. Consequentialist concerns may override respect for informational privacy, but the ontological interpretation, by equating its protection to the protection of personal identity, considers it a fundamental and inalienable right,[14] so that, by default, the presumption should

[10] L. Floridi and J. W. Sanders. Internet Ethics: The Constructionist Values of Homo Poieticus. In Robert Cavalier, editor, *The Impact of the Internet on Our Moral Lives*. SUNY, New York, 2005.

[11] J. Cohen. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, 52: 1373–1437, 2000, p. 1426.

[12] This view is close to the interpretation of privacy in terms of protection of human dignity defended in E. Bloustein. Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review*, 39: 962–1007, 1964.

[13] There is no space here to argue that personal identity ought to be valued morally speaking. Suffice to say that, from an information ethics perspective, this can be treated as a special (both in the sense of specific and of very important) case of the general view according to which the nature of entities and the possibilities of their full development are subject to moral respect (L. Floridi. On the Intrinsic Value of Information Objects and the Infosphere. In *Ethics and Information Technology*, 4(4): 287–304, 2003).

[14] For a different view see R. Volkman. Privacy as Life, Liberty, Property. *Ethics and Information Technology*, 5(4): 199–210, 2003.

always be in favour of its respect, although this of course is not to say that, pragmatically, informational privacy is never negotiable in any degree.

Heuristically, violations of informational privacy are more fruitfully comparable to kidnapping rather than trespassing: the observed is moved to an observer's local space of observation (a space which is remote for the observed), unwillingly and possibly unknowingly. What is abducted is personal information, even though no actual removal of information is in question, but rather only a cloning of the relevant piece of personal information. Yet the cloned information is not a "space" that belongs to the observed and which has been trespassed; it is part of the observed herself, or better something that (at least partly) constitutes the observed for what she or he is.

A further advantage, brought about by this change in perspective, is that it becomes possible to dispose of the false dichotomy qualifying informational privacy in public or in private contexts. Insofar as a piece of information constitutes an agent, it does so context-independently and that is why the observed may wish to preserve her integrity and uniqueness as an informational entity, even when she is in an entirely public place. After all, trespassing makes no sense in a public space, but kidnapping is a crime independently of where it is committed.

Finally, one may still argue that an agent "owns" his or her information, yet no longer in a vaguely metaphorical sense, but in the precise sense in which an agent *is* her or his information. "My" in "my information" is not the same "my" as in "my car" but rather the same "my" as in "my body" or "my feelings": it expresses a sense of *constitutive* and *intimate belonging*, not of external and detachable *ownership*, a sense in which my body, my feelings and my information are part of me but are not my (legal) possessions. As Warren and Brandeis wrote:

> "[...] the protection afforded to thoughts, sentiments, and emotions [...] is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously persecuted, the right not to be defamed [or, the right not to be kidnapped, my addition]. In each of these rights [...] there inheres the quality of being owned or possessed and [...] there may be some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. *The principle* [...] *is in reality not the principle of private propriety but that of inviolate personality* (p. 31, emphasis added) [...] *the right to privacy, as part of the more general right to the immunity of the person*, [is] *the right to one's personality*".[15]

The ontological interpretation stresses that informational privacy is also a matter of construction of one's own informational identity. The right to be let alone is also the right to be allowed to experiment with one's own life, to start again, without having records that mummify one's personal identity forever, taking away from the individual the power to mould it. Everyday, a person may wish to build a different, possibly better, "I". We never stop becoming ourselves, so protecting a person's informational privacy also means allowing that person the freedom to change, ontologically.[16]

Four types of challenges

As anticipated, in this second part of the article I wish to consider a number of challenges that seem to confront any theory of informational privacy. The perspective is metatheoretical: problems concerning informational privacy itself are not under discussion here. The account will not be exhaustive, not merely because this would be impossible, but mainly because it would useless. For the challenges to be taken into account are only those substantial enough to run the risk of undermining a theory of informational privacy, or sufficiently interesting to cast a better light on why a theory is particularly valuable. Since there are several that satisfy these criteria, I shall proceed rather schematically. Finally, no degree of importance should be inferred from the order of presentation, although I shall make an effort to proceed from more general to more specific challenges, and try to link them in a unifying narrative.

Parochial ontologies and non-western approaches to informational privacy

One is often reminded that different cultures and languages may not share similar conceptions of privacy in general, and of informational privacy in particular. Indeed, it has become fashionable to state that privacy is a Western invention of the 18th-century. Thompson,

[15] S. Warren and L.D. Brandeis. The Right to Privacy. *Harvard Law Review*, 193(4): 1890, p. 33, emphasis added.

[16] In this sense, Johnson seems to be right in considering informational privacy an essential element in an individual's autonomy (D.G. Johnson. *Computer Ethics*. Prentice-Hall, Englewood Cliffs, 1985; see also D.G. Johnson. *Computer Ethics*, 3rd ed., Prentice-Hall, Upper Saddle River, NJ, 2001). Moor disagrees (J.H. Moor. Towards a Theory of Privacy in the Information Age. *ACM SIGCAS Computers and Society*, 27: 27–32, 1997).

for example, recalls that "In *The Structure of Everyday Life*, Fernand Braudel states that 'privacy was an 18th-century innovation'; [and that] in *The Structural Transformation of the Public Sphere*, Habermas asserts that the public sphere was an 18th-century invention".[17] Yet this is only partly true, for the history of privacy is far more complex and nuanced, as the monumental work by Ariáes and Duby testifies.[18]

In connection with the suggestion that "privacy" might be a matter (and obsession) limited to Western cultures, global differences may also be unduly emphasised, even when they represent a healthy reminder that no assumption should be too readily made when it comes to such a basic issue.[19] For example, the word "privacy" is certainly imported in Thai[20] and in Japanese,[21] but so it is in other European languages such as Italian or Spanish. And one may easily build a case for a general difference between a Mediterranean and a more northern-European sense of privacy. Such generalizations are often amusing but rarely informative. The truth is that no one would find it reasonable to compare, for example, Eastern and French cuisine. Similar comparisons between over-generic (e.g., Western, Eastern) and more focused (e.g., French, Buddhist, Thai) categories are better left behind, if one wishes to understand what really is at stake.

The difficult solution here seems to navigate between self-deprecation and chauvinism, while avoiding the adoption of some form of more or less hidden relativism, which would merely be synonymous for a substantial failure in achieving a real dialogue. Perhaps the key is a constructive commitment towards the identification and uncovering of those common and invariant traits that unify humanity at all times and in all places. Like "friendship", for example, "privacy" is a slippery concept, which seems to qualify a variety of phenomena that may change from place to place; and yet, this is no argument against its presence in virtually any given culture. In this respect, the ontological theory seems to offer two advantages.

First, instead of trying to achieve an impossible "view from nowhere", the theory seeks to avoid assuming some merely "local" conception of what Western philosophical traditions dictate as "normality" – whether this is understood as post-18th century or not – in favour of a more neutral ontology of entities modelled informationally. By referring to such a "lite" ontological grounding of informational privacy, the theory allows the adaptation of the former to various conceptions of the latter, working as a potential cross-cultural platform. This can help to uncover different conceptions and implementations of informational privacy around the world in a more neutral language, without committing the researcher to a culturally-laden position.

Second, since the ontological theory of privacy relies on an informational ontology, it may more easily resound with a humanity that is increasingly used to the re-ontologising impact of global ICTs. Teenagers from all over the world are nowadays more likely to communicate by relying on their shared experiences with online entertainments, for example, than by referring to their parents' conceptions of reality based on dolls and plastic figures of WWII soldiers. In a few generations, an informational ontology will seem obvious to the point of being trivial. This is not to say that a global and uniform sort of digitally pasteurized culture will be drowning on us any time soon. As Saussure clearly demonstrated with respect to languages, diachronic forces of appropriation and re-appropriation inevitably articulate, particularise and localize any apparently global trend. No universal language or culture should be expected to arise across all the various information societies around the world. However, in the same way as people will increasingly often speak not only their own idioms and natives dialects but also some form of basic English good enough to communicate with each other, likewise, an informational ontology will probably represent the shared *koiné* among future netizens.

Individualism and the anthropology of informational privacy

Western alleged "individualism" may be seen as a specific form of parochialism, determined by a deeply ingrained and yet utterly contingent anthropology obsessed with individuals, their needs and desires, their egotisms, and their market-driven, cost-benefit-oriented, logo-centric behaviours. The latter is a caricature and a rather unsophisticated one at that, I concede, but it is not too far from a decent sketch of some culturally-shortsighted and mono-ethnic work that circulates even in some applied studies of computer ethics. The broad challenge here is whether there

---

[17] J. Thompson. *Models of Value: Eighteenth-Century Political Economy and the Novel*. Duke University Press, Durham, N.C., London, 1996, p. 29.

[18] P. Ariáes and G. Duby. *A History of Private Life*, 5 vols. Belknap Press of Harvard University Press, Cambridge, Mass, London, 1987.

[19] On this see C. Ess, editor, *Special Issue on Privacy and Data Privacy Protection in Asia* (Ethics and Information Technology), 2005.

[20] K. Kitiyadisai. Privacy Rights and Protection: Foreign Values in Modern Thai Context. *Ethics and Information Technology*, 7(1): 17–26, 2005.

[21] M. Nakada and T. Tamura. Japanese Conceptions of Privacy: An Intercultural Perspective. *Ethics and Information Technology*, 7(1): 27–36, 2005.

can be any sense in talking of a theory of informational privacy without the private subject, to paraphrase the title of a famous paper by Popper on epistemology without the knowing subject. My short answer is negative: informational privacy requires a privacy holder, but with a crucial qualification.

What most critics of "individualism" seem to oversee, perhaps blinded by an understandable eagerness to redress the situation, is that the concept of "individual" is not the same as the concepts of "person", "subject", "agent", "mind", "soul" or "self". All these can be used interchangeably, of course, and not necessarily mistakenly so. But when some generic allusion is made to the alleged absence of any concept of any sort of individuality in non-Western cultures or philosophies, or when theories of privacy (including the informational variety) are criticised for being oblivious of the patent lack of any privacy holders in some non-Western countries, then the ethicist needs to reach for his finest pencil, and re-draw some distinctions, even at the risk of being pedantic.

First, facts are not norms: if things are such that a culture, a legislation or a philosophy lacks any conception of a privacy holder, this is no reason to argue that it should not acquire one. A specific example may help. It is well known that Article 12 of the Universal Declaration of Human Rights states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[22] Now the Declaration was adopted in 1948 by the General Assembly of the United Nations, and that date might be taken as the beginning of a universal theory of privacy, not limited to Western countries and cultures. However, the African (Banjul) Charter on Human and Peoples' Rights, adopted in 1981 by the OAU,[23] which is quite clearly modelled on the Universal Declaration, contains no reference to privacy or cognate concepts. From a normative point of view, it seems that this is a shortcoming, that the shortcoming is suspicious, and that it would be good if the Charter could be amended. The document does not prove that it is ethically acceptable that privacy rights in Africa should not be recognised.

Second, there are main-stream and influential traditions, within Western cultures and philosophies, that value (when not privilege) the community over the individual. Space here allows only for a few quick reminders. Greek and Roman philosophies are primarily social, to the extent that they defended the role of the *polis* and of the *res publica* as the real contexts where someone becomes oneself. Christianity is intrinsically ecclesiastical[24] and Judaism congregational (God relates to the whole people of Israel). The very concept of democracy takes something away from the individual to emphasise the centrality of the "multi-agent" system. It would be easy to add other examples.

What goes under the label of "Western individualism" is to be understood not so much in terms of the centrality of the single self, but rather in terms of the raising of a sense of personal responsibility, which co-develops with political activities (Greece), legal systems (Rome), religious beliefs (Judaism/Christianity) and epistemic practices (Scientific Revolution) and is often supposed to be monitored by an omniscient God, who can see everything you do better than any omniscient Big Brother ever imagined.[25]

This leads to a third point: personal responsibility is not unknown to other cultures. If I may be allowed to draw some more caricatures: in many non-Western cultures or religions it is up to the *individual* to see that he or she reincarnates into, or transmigrates to, higher forms of life. And responsibility is not "dispersed" in a vaporous sense of fuzzy subjectivity if you feel the pressure of committing suicide for having failed, again, as an *individual*, to uphold certain standards or fulfil some expectations, or if you are invited, as an embodied and embedded agent, to annihilate your subjectivity, which therefore must be there in the first place.[26] Not every philosophy of the subject is subjectivist, nor every philosophy of the "I" is also a philosophy of the "me", and not every philosophy that talks of agents is necessarily committed to the existence of substantial selves. Yet a lot of bad press concerning poor Monsieur Descartes, for example, takes advantage of such confusions. Where there is personal responsibility there is also an individual capable of shouldering it, but then there is some conception of a single human being, different from society, capable of desiring some form of privacy for his or her own life.

Superficial contrasts between Western and non-Western cultures both trivialise ostensible differences and obscure important commonalities, distorting central notions of the individual and of individual

[22] http://www.un.org/Overview/rights.html

[23] http://www.africa-union.org/

[24] "Ecclesia" simply meant "assembly" in Greek, etymologically "the body of the select counsellors". Solon originally coined it as the name given to the public formal assembly of the Athenian people.

[25] For "His eyes are on the ways of men; he sees their every step" (Job 34:21) and he "knows what you need before you ask him" (Mt 6:8,32).

[26] S. Hongladarom. Analysis and Justification of Privacy from a Buddhist Perspective. In S. Hongladarom and C. Ess, editors, *Information Technology Ethics: Cultural Perspectives*. Idea Publishing, Hershey, Pennsylvania, 2006.

responsibility. It seems it is high time to reshelve supermarket spiritualism where it belongs, i.e., the department of astrology, comfort food and Western parochialism.

The ontological theory of informational privacy can help in this process in that it does not presuppose either a personalist or a substantialist conception of the agents involved in moral actions. Agents need not be persons, they can be organizations, for example, or artificial constructs, or hybrid syntheses. And they do not need to consist of some self-like sort of entities, as they may be constituted by bundles of properties and processes. Once again, this "lite" ontology can be adapted to further interpretations and cultural needs. It helps to be able to frame the discussion in a minimalist way that does not exclude a priori some interlocutors.

The scope and limits of informational privacy

Under this heading it is useful to list a family of problems that highlight how some theories end up either shrinking or inflating the concept informational privacy.

First, there are some insightful and conclusive criticisms to Rachels and Fried, moved by Reiman in the context of his broader criticism of Thomson and her "ownership" theory of informational privacy.[27] According to what Reiman labels the Rachels-Fried theory,

> "Only because we are able to withhold personal information about – and forbid intimate observation of – ourselves from the rest of the world, can we give out the personal information – and allow the intimate observations – to friends and/or lovers, that constitute intimate relationships. On this view, intimacy is both signalled and constituted by the sharing of information and allowing of observation *not shared with or allowed to the rest of the world*. If there were nothing about myself that the rest of the world did not have access to, I simply would not have anything to give that would mark off our relationship as intimate."[28]

Intimacy is certainly an important aspect of informational privacy.[29] Yet, Reiman rightly argues that a "market-oriented" analysis of privacy as a sort of intimacy-purchasing currency ("moral capital", in Fried's terminology) is both contingent on what has been defined above as a form of parochialism (the market orientation of values, in this case) and undermined by a logical fallacy.

If things were as the Rachels-Fried theory suggests, then people would be most intimate with e.g., doctors, lawyers, psychoanalysts or priests, with whom they share all sort of personal information they would not dare to share with anyone else, including those with whom they are actually most intimate. Yet this is absurd. For I agree with Reiman that the real difference is made by the relation of *caring*, not by the mere amount or type of information exchanged. And it is precisely the relation of caring that regulates what and how much information one is willing to share with someone with whom one enjoys an intimate relation. It is well known that sometimes one can speak more freely with a stranger precisely because there is very little intimacy, and not in view of establishing any.

Furthermore, anyone intrinsically unable to enter in any social relation – like a comatose or seriously mentally ill person (recall the example of the patients in the hospital ward) – would be *de facto* deprived of any informational privacy, since the latter is made to be dependent on the former,[30] in the same sense in which some old banknotes, that cease to be legal tender, can no longer be used to purchase any good. Allegedly, "privacy creates the moral capital which we spend in friendship and love."[31] But if you can no longer be a customer, you do not need it.

---

[27] J.H. Reiman. Privacy, Intimacy, and Personhood. *Philosophy and Public Affairs*, 6(1): 26–44, 1976; J. Rachels. Why Privacy Is Important. *Philosophy and Public Affairs*, 4: 323–333, 1975; C. Fried. *An Anatomy of Values: Problems of Personal and Social Choice*. Harvard University Press, Cambridge, Mass, 1970. Thomson is also criticised by Scanlon (T. Scanlon. Thomson on Privacy. *Philosophy and Public Affairs*, 4: 315–322, 1975), while Rachels criticises both (J. Rachels. Why Privacy Is Important. *Philosophy and Public Affairs*, 4: 323–333, 1975). Reiman, coming last in the debate, is able to show the shortcomings of all three. Introna seems to agree with, and update, Reiman's position, if from a more Foucaultian perspective (L.D. Introna. Privacy and the Computer: Why We Need Privacy in the Information Society. *Metaphilosophy*, 28(3): 259–275,1997) while Johnson seeks to reconcile Benn's Kantian approach to privacy in terms of protection of selfhood with Reiman's care-oriented approach (J.L. Johnson. A Theory of the Nature of Value of Privacy. *Public Affairs Quarterly*, 6(3): 271–288, 1992; S. I. Benn. Privacy, Freedom, and Respect for Persons. In Richard Wasserstrom, editor, *Today's Moral Problems*. Macmillan, New York, 1975). A very valuable contribution is provided by Cohen (J. Cohen. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, 52: 1373–1437, 2000), who develops a clear and sharp criticism of theories of informational privacy based on the concepts of ownership, control/choice and freedom of speech. The article is particularly interesting as it shows how such interpretations of informational privacy may "fire back" and allow, if adopted, solid reasons in favour of a more relaxed attitude and market-friendly attitude towards personal data processing, especially in the US.

[28] J.H. Reiman. *Privacy, Intimacy, and Personhood*, pp. 31–32.

[29] J.C. Inness. *Privacy, Intimacy, and Isolation*. Oxford University Press, New York, 1996.

[30] J.H. Reiman. *Privacy, Intimacy, and Personhood*, p. 36.

[31] C. Fried. *An Anatomy of Values: Problems of Personal and Social Choice*, p. 25.

Rachels and Fried fail to take into account forms of informational privacy that we would like to consider both genuine and important. But others may end up inflating the concept of informational privacy in ways that turn out to be unrealistic (things stand differently) and then vacuous (nothing counts as privacy-unrelated). This is the case when *any* informational process concerning a person becomes a breach of that person's informational privacy. Again, Reiman provides an early and very valuable analysis of this sort of problem in his lucid criticism of Benn. Let me illustrate it by using an everyday example.

Imagine that John and Peter are neighbours. If the former sees the latter's car parked outside the house, a theory of informational privacy needs to able to avoid counting this as necessarily a case of privacy breach. The same holds true for the case in which Peter drives away at a certain time in the afternoon and, without him knowing it, he is inadvertedly seen by John, who is doing some gardening. If all cases of access to information about someone become cases of infringement of the informational privacy of that someone, we merely erase the conceptual distinction between being informed about someone's business and infringing someone's informational privacy and hence deprive ourselves of the possibility of explaining when the former does not amount to the latter and what ought to be done when it does. A theory of informational privacy needs a criterion of discrimination to be able to explain why some information processes do *not* count as violations of privacy.

A third difficulty of "scope", affecting several theories of informational privacy based on some version of personal information ownership/control, concerns inferential processes. Consider our simple example. Suppose Peter is informed that, if John leaves the house, John's wife, Mary, remains alone in the house. Imagine next that Peter sees John driving away and Mary going back into the house. He is therefore informed that Mary is alone in the house. Information is closed under entailment, as logicians like to say. So seeing John driving away triggers a process that ends by breaching Mary's privacy. Now, what interests us here is the opposite process. Precisely because one may infer from John's absence Mary's state as the only person in the house, where does Mary's ownership of, or right to control "information about herself" end? It seems it should include John's localization as well. This generates a cascade of further difficulties, two of which are worth stressing.

On the one hand, there is a collapse of the naïve idea that information I about a group of people S might be easily partitioned into a finite set of disjoint pieces of information $\{I_1, ..., I_n\}$ about the individuals $\{i_1, ..., i_n\}$ constituting S, whose union is I. In other words, a lot of personal information overlaps and covers many people at once: information about John's absence is information about Mary's solitude in the house, and vice versa, so these pieces of information cannot be merely owned or controlled by either John or Mary disjointly. This calls for a refined theory of control closure among distributed systems.[32]

On the other hand, speaking of co-ownership or shared control of personal information becomes meaningless once it is clear that – even if semantic information is defined as embedding truth ("false information" merely means "not information"[33]) – there is still an endless amount of information that can be inferred (and hence retro-engineered) starting from some initial information. Inferential closure plus co-ownership or shared control make the concept of "personal information" too foggy to be of much use and applicability.

How the ontological theory of informational privacy avoids these difficulties may be explained in the following terms.

Anyone defending the following two theses:

(a) that false information is genuine information; and
(b) that informational privacy is based on ownership/control of information about oneself;

is also forced to conclude that, since

(c) "being informed" is closed under implication, then
(d) any informational process whatsoever is an infringement of one's informational privacy.

Yet, this is a *reductio ad absurdum*. And if one seeks to avoid it by weakening condition (a) into:

a*) only "true" information is genuine information,and condition (c) into:

c*) inferential closure may fail

sometime,this is still insufficient to make (d) reasonably constrained. There still remain an awfully huge amount of information that seems to belong to individuals exclusively, and should fall under their personal control. The only way out is to drop (b), but this is exactly what the ontological theory of informational privacy does. Agents do not own their information but are constituted by it.

[32] See M. Turilli. Ethical Protocols Design, *Ethics and Information Technology*, forthcoming.

[33] See L. Floridi. Is Information Meaningful Data? *Philosophy and Phenomenological Research*, 70(2): 351–370, 2005 and L. Floridi. The Logic of Being Informed. *Logique et Analyse*, forthcoming.

Public, passive and active informational privacy

It may seem an oxymoron but a theory of informational privacy should be able to explain and support ''public informational privacy'', i.e., privacy in public, as Nissenbaum and Margulis have convincingly argued.[34]

The difficulty here is represented by the need to abandon some naïve conceptions of privacy in terms of metaphorical private versus public ''spheres''. Contrary to what intuition may initially dictate, by moving in and out of the ''public sphere'' (e.g., by going to the pub or staying home) an agent is not *ipso facto* readjusting, each time, the degree of informational privacy to which he has a justified claim, but only the degree of informational privacy of which he or she can have a reasonable expectation. Many people who would be embarrassed to show themselves naked in front of strangers, find showering at the gym with other unknown members unproblematic. The degree of informational privacy one may enjoy is patently determined also by the social context, as we have seen in the first part of the article, but it should not be confused with it. Likewise, there is of course a difference between private (non-public) personal information, which might be highly sensitive, such as one's own medical records, and public personal information, which is not necessarily confidential or intimate, such as one's own gender, race and ethnic group. And in public, one's informational privacy is more easily at stake than in private, obviously. But the fragility of one's informational privacy in public and of one's public personal information – both so easily subject to computerised processing (gathering, exchanging, mining, matching, merging etc.) – is a fundamental reminder that we should be more and not less concerned about the phenomenon of ''public privacy''. After all, recent American and European history is full of tragic abuses of ''public information.''[35]

The reader may recall that the ontological theory tackles this difficulty by comparing privacy to other rights such as personal safety. One has a right to personal safety both in private and in public, although, in public contexts, expectations that this right will be respected might be much lower than in private contexts.

We have already encountered what I have called ''passive informational privacy'', when discussing the need for a theory to account for, and safeguard, one's profile as an informational entity not only from operations of cloning in public but also from attempts at corruption, again, especially in the public sphere. Providing someone with some information may easily mean violating that person's informational privacy, in two senses.

On the one hand, each of us has a fundamental right not to know: that is why violent scenes, disturbing news, pornography, advertising, unwanted reports or spoilers (the final of the world cup is over but one does not wish to know the result in order to enjoy it later on TV) and, I may add, mere idiocy, of which there is an overabundance throughout all media, may be suffered as contaminations of one's own self, as breaches of one's own informational privacy, brain washing of the worst kind.

On the other hand,[36] each of us has a fundamental duty to ignore (or pretend not to know): in human societies privacy is also fostered through tacit agreements. We ''politely'' ignore – e.g., do not bring up in conversation – moments we all witness and know about, ranging from keeping our eyes straight ahead at the urinal to never speaking of, say, marital acts that we know (and sometimes have evidence to confirm) must take place, etc. Again, no theory of informational privacy is complete that cannot account for such phenomena.

Finally, by ''active informational privacy'' in the public sphere I mean to refer to those practices that facilitate and foster the development of individuals, by guaranteeing relevant conditions of informational privacy construction. What the latter may be varies from culture to culture and through time, but it seems quite clear that the right to informational privacy is not merely a negative right not to be x-ed, but also a positive right to x-ing. Parents know this too well when they decide that their children's rooms, or that space in the tree house, are off-limits. It is respect for such conditions of possibility of other's informational privacies that mark the presence of that *caring* attitude already highlighted above.

Conclusion

By way of conclusion I would like to offer two last comments. One concerns non-informational kinds of privacy. It is common to distinguish between *accessibility privacy*, understood as the freedom from

[34] H. Nissenbaum. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17(5–6): 559–596, 1998; S.T. Margulis. Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues*, 59(2): 243–261, 2003.

[35] W. Seltzer and M. Anderson. The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses. *Social Research*, 68(2): 339–371, 2001.

[36] I owe this insight entirely to Charles Ess, who called my attention to this important aspect.

intrusion and/or the right to be left alone in one's own physical space, and *decisional privacy*, understood as the freedom from interference in one's own choices and decisions or the right to determine one's own course of actions, especially in relation to sexual options and reproductive alternatives.[37] Now, it seems natural to expect that theories of informational privacy, once mature, will make a sincere and robust effort to coordinate their findings and conclusions with those of other theories of other forms of privacy, in order to gain a comprehensive and coherent view of privacy in all its major aspects. And yet this seems an area largely unexplored. As usual, talking of Wittgensteinian family resemblances[38] only helps to postpone the problem: for those who stress the differences will then concentrate on the mere "resemblance", whereas those who stress the similarities will keep looking for the common traits.

The second observation concerns a lower level of analysis. In this paper, I have been concerned with challenges concerning a theory of informational privacy. Moving from this metalevel to the object level of problems regarding informational privacy itself, I would like to suggest that, depending on one's theory, some practical difficulties may be turned into hermeneutic opportunities, providing a metaphorical keyhole through which one may look at other phenomena otherwise difficult to investigate. By this I mean that the careful study of privacy infringements may provide an indirect method to probe whatever lies behind it, if anything, much like the study of unhealthy brains may help to understand the proper functioning of healthy ones. This is generally true of any theory that reduces or (more moderately) relates informational privacy to some other phenomena. For example, a theory that interprets informational privacy in terms of ownership/control will also be able to understand the latter more accurately by studying the pathology of the former. In our case, if informational privacy is indeed strictly connected to personal identity – as the ontological theory advocates – then the study of its pathology, i.e., of informational privacy breaches, will offer valuable insights into the nature and dynamics of personal identity itself. In both cases, as far as the ontological theory is concerned, this is work left to the future.

[37] M. Schachter. *Informational and Decisional Privacy*. Carolina Academic Press, Durham, N.C., 2003.

[38] D.J. Solove. Conceptualizing Privacy. *California Law Review*, 90: 1087–1155, 2002.

Acknowledgements

This paper is a fully revised version of a presentation given at the international workshop "Bridging Cultures: Computer Ethics, Culture, and ICT", organised by the Programme for Applied Ethics in association with the Globalisation programme at NTNU (the Norwegian University of Science and Technology, Trondheim, Norway, June 6th–7th 2005). For that opportunity and for the feedback received, I wish to thank Charles Ess and May Thorseth (co-organisers), Eric Monteiro, Knut Rolland, Johnny Søraker, Bernd Carsten Stahl, Deborah Wheeler and all the students who took part to the workshop, and, for the financial support, NTNU. Charles Ess shared with me some important insights while discussing the final draft, and I hope I managed to take full advantage of his suggestions. As usual, all remaining mistakes are unfortunately mine.

References

P. Ariáes and G. Duby, *A History of Private Life,* 5 vols. Belknap Press of Harvard University Press, Cambridge, Mass, London, 1987.

I. Asimov. The Dead Past. In *Astounding Science Fiction*, 6–46, 1956. manca qualche informazione, no?.

E. Bäck and K. Wikblad. Privacy in Hospital. *Journal of Advanced Nursing*, 27(5): 940–945, 1998.

S.I. Benn. Privacy, Freedom, and Respect for Persons. In Richard Wasserstrom, editor, *Today's Moral Problems*. Macmillan, New York, 1975.

E. Bloustein. Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review*, 39: 962–1007, 1964.

J. Cohen. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, 52: 1373–1437, 2000.

C. Ess, editor, *Special Issue on Privacy and Data Privacy Protection in Asia* (Ethics and Information Technology), 2005.

L. Floridi On the Intrinsic Value of Information Objects and the Infosphere. In *Ethics and Information Technology*, 4(4): 287–304, 2003.

L. Floridi Is Information Meaningful Data? In *Philosophy and Phenomenological Research* 70(2): 351–370, 2005.

L. Floridi. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, 7(4): 185–200, 2005.

L. Floridi, Information Ethics. In Jeroen van den Hoven and John Weckert, editors, *Moral Philosophy and Information Technology*, Cambridge University Press, Cambridge, forthcoming.

L. Floridi. The Logic of Being Informed. *Logique et Analyse*, forthcoming.

L. Floridi and J.W. Sanders. On the Morality of Artificial Agents. *Minds and Machines*, 14(3): 349–379, 2004.

L. Floridi and J.W. Sanders.. Internet Ethics: The Constructionist Values of Homo Poieticus. In Robert Cavalier, editor, *The Impact of the Internet on Our Moral Lives*. SUNY, New York, 2005.

C. Fried, *An Anatomy of Values: Problems of Personal and Social Choice*. Harvard University Press, Cambridge, Mass, 1970.

J.J. Gibson, *The Ecological Approach to Visual Perception*. Houghton Mifflin, Boston, London, 1979.

S. Hongladarom. Analysis and Justification of Privacy from a Buddhist Perspective. In S. Hongladarom and C. Ess, editors, *Information Technology Ethics: Cultural Perspectives*. Idea Publishing, Hershey, Pennsylvania, 2006.

J.C. Inness, *Privacy, Intimacy, and Isolation*. Oxford University Press, New York, 1996.

L.D. Introna. Privacy and the Computer: Why We Need Privacy in the Information Society. *Metaphilosophy*, 28(3): 259–275, 1997.

D.G. Johnson, *Computer Ethics*. Prentice-Hall, Englewood Cliffs, 1985.

D.G. Johnson, *Computer Ethics,* 3rd ed. Prentice-Hall, Upper Saddle River, NJ, 2001.

J.L. Johnson. A Theory of the Nature of Value of Privacy. *Public Affairs Quarterly*, 6(3): 271–288, 1992.

K. Kitiyadisai. Privacy Rights and Protection: Foreign Values in Modern Thai Context. *Ethics and Information Technology*, 7(1): 17–26, 2005.

S.T. Margulis. Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues*., 59(2): 243–261, 2003.

J.H. Moor. Towards a Theory of Privacy in the Information Age. *ACM SIGCAS Computers and Society*, 27: 27–32, 1997.

M. Nakada and T. Tamura. Japanese Conceptions of Privacy: An Intercultural Perspective. *Ethics and Information Technology*, 7(1): 27–36, 2005.

H. Nissenbaum. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17(5–6): 559–596, 1998.

J. Rachels. Why Privacy Is Important. *Philosophy and Public Affairs*, 4: 323–333, 1975.

J.H. Reiman. Privacy, Intimacy, and Personhood. *Philosophy and Public Affairs*, 6(1): 26–44, 1976.

T. Scanlon. Thomson on Privacy. *Philosophy and Public Affairs*, 4: 315–322, 1975.

M. Schachter, *Informational and Decisional Privacy*. Carolina Academic Press, Durham, N.C, 2003.

W. Seltzer and M. Anderson. The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses. *Social Research*, 68(2): 339–371, 2001.

D.J. Solove. Conceptualizing Privacy. *California Law Review*, 90: 1087–1155, 2002.

J. Thompson, *Models of Value: Eighteenth-Century Political Economy and the Novel*. Duke University Press, Durham, N.C. London, 1996.

J. Thomson. The Right to Privacy. *Philosophy and Public 957 Affairs*, 4: 295–314, 1975.

M. Turilli. Ethical Protocols Design, *Ethics and Information Technology*, forthcoming.

R. Volkman. Privacy as Life, Liberty, Property. *Ethics and Information Technology*, 5(4): 199–210, 2003.

S. Warren and L.D. Brandeis. The Right to Privacy. *Harvard Law Review*, 193(4), 1890.