Preprint from http://www.wolfson.ox.ac.uk/~floridi/

This paper has been accepted for publication in

Computers & Society

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

It is a publisher's requirement to display the following notice:
The documents distributed by this server have been provided by the contributing authors as a means to ensure timely dissemination of scholarly and technical work on a noncommercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that they have offered their works here electronically. It is understood that all persons copying this information will adhere to the terms and constraints invoked by each author's copyright. These works may not be reposted without the explicit permission of the copyright holder.

Valeria Giardino

Digitally signed by Valeria Giardino
DN: CN = Valeria Giardino, C = IT, O = Universita' di Roma La Sapienza, OU = Dipartimento di Logica ed Epistemologia
Reason: I attest to the accuracy and integrity of this document
Date: 2006.05.02 15:54:07 +02'00'

Informational Privacy and Its Ontological Interpretation

Luciano Floridi[1,2,3]
[1]Dipartimento di Scienze Filosofiche, Università degli Studi di Bari; [2]Faculty of Philosophy and [3]Information Ethics Group, OUCL, Oxford University.
Address for correspondence: Wolfson College, OX2 6UD, Oxford, UK; luciano.floridi@philosophy.oxford.ac.uk

Introduction

The article provides an outline of the ontological interpretation of informational privacy based on information ethics (Floridi [forthcoming-b]). It is part of a larger project of research, in which I have developed the foundations of ideas presented here (Floridi [forthcoming-c]) and their consequences (Floridi [forthcoming-a])

As an outline, it is meant to be self-sufficient and to provide enough information to enable the reader to assess how the approach fares with respect to other alternatives. However, those interested in a more detailed analysis, and especially in the reasons offered in its favour, may wish to consult the other articles as well.

A simplified model

Let me start by introducing a simplified model of a situation in which informational privacy might be at stake. Imagine a limited (region of the) *infosphere*, represented by some patients (our interactive, informational agents) admitted to the same hospital (our limited environment (for an empirical assessment see Bäck and Wikblad [1998]).

Infosphere is a neologism I coined years ago on the basis of "biosphere", a term referring to that limited region on our planet that supports life. It denotes the whole informational environment constituted by all informational entities (thus including informational 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 includes also off-line and analogue spaces of information.

Intuitively, given a certain amount of available information somewhere in the infosphere, 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 among the agents may be described as 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 protect. Thus, the ontological features of the infosphere determine a specific degree of *ontological friction* regulating the information flow within the system.

By ontological friction I mean to refer 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 and memory), amount and complexity of the data to be processed, and so forth.

Of course, the informational affordances 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.

Let me now summarize the previous analysis. What we have seen is that, 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.

ICT as re-ontologizing technologies

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 (Moor [1997] highlights a similar point "When information is computerised, it is *greased* to slide easily and quickly to many ports of call" (p. 27). 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* the very nature of the infosphere, that is, of the environment itself, of the agents embedded in it and of their interactions. *Re-ontologizing* is another neologism that I have recently coined in order to refer to a very radical form of re-engineering, one that not only designs, constructs or structures a system (e.g. a company, or a machine) anew, but that fundamentally transforms its intrinsic nature. In this sense, for example, nanotechnologies and biotechnologies are not merely re-engineering but actually re-ontologizing our world.

Digital ICTs are *re-ontologizing devices* because they engineer new environments that the user/agent is then enabled to inhabit. Imagine, for example, 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. In "The Dead Past" Asimov [1956] describes a *chronoscope,* a device that allows direct observation of past events. The chronoscope turns out to be of only limited use for archaeologists, since is can look only

a couple of centuries in the past, but people discover that it can easily be tuned to the most recent past, with a granularity of fractions of seconds before. 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.

These thought experiments illustrate how radical modifications in the very nature (that is to say, a re-ontologization) of the infosphere can dramatically change the conditions of possibility of informational privacy.

To summarise: informational privacy is a function of the ontological friction in the infosphere. Many factors can affect the latter, including, most importantly, *technological innovations* and *social developments*. 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. On the contrary, 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.

Privacy in the infosphere

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 but also *poietic* (i.e. constructive) applications, which

may allow users to design, shape and maintain their identities as informational agents (Floridi and Sanders [2005]). 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 (even a utopian one) 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 that may be advocated by some– recall the example of the glassy hospital and of our mentally super-enhanced patients – 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. As Cohen [2000] has 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." (p. 1426).

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, either actively – collecting, storing, reproducing, manipulating etc. one's information amounts now to stages in stealing, cloning or breeding someone else's personal identity – or passively – as 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 (This view is close to the interpretation of privacy in terms of protection of human dignity defended by Bloustein [1964]). 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 he right to informational privacy (both in the active and in the passive sense just seen) shields one's personal identity. 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 (for a different view see Volkman [2003]), so that, by default, the presumption should always be in favour of its respect (this of course is not to say that 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 and no actual removal is in question, but 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 [1890] 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* (p. 33, emphasis added).

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. In this sense, Johnson [2001] seems to be right in considering informational privacy an essential element in an individual's autonomy (Moor [1997], referring to a previous edition of Johnson [2001], disagrees).

References

Asimov, I. 1956, "The Dead Past", *Astounding Science Fiction*, 6-46.

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

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

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

Floridi, L. forthcoming-a, "Four Challenges for a Theory of Informational Privacy", *Ethics and Information Technology*.

Floridi, L. forthcoming-b, "Information Ethics" in *Moral Philosophy and Information Technology*, edited by Jeroen van den Hoven and John Weckert (Cambridge: Cambridge University Press),

Floridi, L. forthcoming-c, "The Ontological Interpretation of Informational Privacy", *Ethics and Information Technology*.

Floridi, L., and Sanders, J. W. 2005, "Internet Ethics: The Constructionist Values of Homo Poieticus" in *The Impact of the Internet on Our Moral Lives*, edited by Robert Cavalier (New York: SUNY),

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

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

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