Ethics and Information Technology (2005) 7:185–200
DOI 10.1007/s10676-006-0001-7

The ontological interpretation of informational privacy

Luciano Floridi
Dipartimento di Scienze Filosofiche, Università degli Studi di Bari, Bari, Italy; Faculty of Philosophy and Information Ethics Group, OUCL, Oxford University, Oxford, UK; Wolfson College, OX2 6UD, Oxford, UK
E-mail: luciano.floridi@philosophy.oxford.ac.uk

Abstract. The paper outlines a new interpretation of informational privacy and of its moral value. The main theses defended are: (a) informational privacy is a function of the ontological friction in the infosphere, that is, of the forces that oppose the information flow within the space of information; (b) digital ICTs (information and communication technologies) affect the ontological friction by changing the nature of the infosphere (re-ontologization); (c) digital ICTs can therefore both decrease and protect informational privacy but, most importantly, they can also alter its nature and hence our understanding and appreciation of it; (d) a change in our ontological perspective, brought about by digital ICTs, suggests considering each person as being constituted by his or her information and hence regarding a breach of one's informational privacy as a form of aggression towards one's personal identity.

Key words: information ethics, informational privacy, infosphere, ontological friction, personal identity

Introduction

"'One of these days d'you think you'll be able to see things at the end of the telephone?' Peggy said, getting up." She will not return to her wondering again, in the remaining pages of Virginia Woolf's *The Years*. The novel was published in 1937. Only a year earlier, the BBC had launched the world's first public television service in London, and Alan Turing had published his groundbreaking work on Turing Machines (Turing, 1936).

Distracted by a technology that invites practical usage more readily than critical reflection, Peggy only half-perceives that new ICTs (information and communication technologies) are transforming society profoundly and irrevocably. The thirties were laying the foundations of the information society. It was difficult to make complete sense of such a significant change in human history, at this early stage of its development. Nevertheless, an evocative phrase concerning the topic of this article appears in an essay on Montaigne, again by Virginia Woolf (*The Common Reader*, 1925): "[we], who have a private life and hold it infinitely the dearest of our possessions [...]", will find protecting it ever more difficult in a social environment increasingly dependent on Peggy's futuristic technology.

Today, the commodification of ICTs, begun in the seventies, and the consequent spread of a global information society since the eighties, are progressively challenging the right to informational privacy, at least as westerners still conceived it in Virginia Woolf's times. The problem is pressing.[1] It has prompted a stream of scholarly and scientific investigations, witness this special issue of *Ethics and Information Technology*; and there has been no shortage of political decisions and legally enforceable measures to tackle it.[2] The goal of this paper, however, is not to review the very extensive body of literature dedicated to informational privacy and its legal protection, even in the relatively limited area of computer ethics studies. Rather, it is to argue in favour of a new ontological interpretation of informational privacy and of its moral value, on the basis of the conceptual frame provided by Information Ethics (Floridi, 1999; forthcoming-a).

Informational privacy and computer ethics

Why have digital ICTs made informational privacy one of the most obvious and pressing issues in computer ethics? The question is crucial[3] and deceptively simple.

[1] Especially in the US, see Garfinkel (2000).

[2] Froomkin (2000) still provides a valuable review.

[3] See for example Johnson (2001), Bynum and Rogerson (2004) and Tavani (2003).

According to one of the most widely accepted explanations, digital ICTs exacerbate old problems concerning informational privacy because of the dramatic increase in their data *Processing* capacities, in the speed (or *Pace*) at which they can process data, and in the *Quantity* and *Quality* of data that they can collect, record and manage. This can be referred to as the 2P2Q hypothesis.

The trouble with any approach sharing the 2P2Q hypothesis is that it concentrates only on obvious and yet secondary effects of the *digital* revolution, and that it does so from a "continuist" philosophy of technology (more on this later). It thus fails to account for the equally important fact that digital ICTs are also responsible both for a potential *increase* in some kinds of informational privacy and, above all, for a radical *change* in its overall nature. ICTs are more redrawing rather than erasing the boundaries of informational privacy. A few examples may help to illustrate the point. Consider

- the "remotization" of information management, such as the ordinary phenomenon of booking, banking or shopping online;
- the growth of anonymous, indirect or non-personal interactions. According to a recent survey by Freever (a mobile-services firm, http://www.freever.com) 45% of Britons had lied about their location by text message; this is privacy as well;
- the much faster and more widespread revisability, volatility and fragility of digital data. Personal records can be upgraded or erased at the stroke of a key, destroyed by viruses in a matter of seconds, or become virtually unavailable with every change in technological standards, whereas we are still able to reconstruct whole family trees thanks to parish documents that have survived for centuries; or
- the various technologies that enable users to encrypt, firewall or protect information (e.g. with passwords or PIN).

In each case, it seems that digital ICTs allow both the erosion of informational privacy and its protection. The following, colourful episode is indicative: "Hong Kong businessmen, for example, once did not dare to leave their mobile phones switched on while visiting sleazy Macau, because the change in ringing tone could betray them. After the ringing tone for Macau was changed to sound like Hong Kong's, however, they could safely leave their phones on, and roaming revenues soared." (*The Economist*, December 2nd 2004).

2P2Q explains only half of the story.

The new challenges posed by digital ICTs are not only a matter of "more of the same". They have their roots in a radical and unprecedented transformation in the very nature (ontology) of the informational environment, of the informational agents[4] embedded in it and of their interactions. As will be argued in this article, understanding this ontological transformation provides a better explanation that is not only consistent with the 2P2Q hypothesis – now to be interpreted as a mere secondary effect of a far more fundamental change – but also closer to the kernel of the privacy problem in the information society.

Informational privacy as a function of ontological friction

Imagine a model of a limited (region of the) infosphere, represented by four students (our set of interactive, informational agents) living in the same house (our limited environment). Intuitively, given a certain amount of available information (which can be treated as a constant and hence disregarded), 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 our example, there will be more or less informational privacy depending on whether the students are allowed, e.g., to have their own rooms and lock their doors. Other relevant conditions are easily imaginable (individual fridges, telephone lines in each room, separate entrances, etc.).

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 walls in the house are few and thin and all the students have excellent hearing, the degree of accessibility is increased, the informational gap is reduced and informational privacy is more difficult to obtain and protect. The love life of the students may be deeply affected by the Japanese-style house they have chosen to share.

The ontological features of the infosphere determine a specific degree of "ontological friction" regulating 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 required for a certain kind of agent to obtain information (also, but not only) about other agents in a given environment, e.g. by establishing and

[4] For a precise definition of agent see Floridi and Sanders (2004b).

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 etc.

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 provide much higher "ontological friction" for the flow of acoustic information than a paper-thin partition, but this is irrelevant if the students are deaf. More realistically, the debate on privacy issues in connection with the design of office spaces (from private offices to panel-based open plan office systems, to completely open working environments, see Becker and Sims (2000)) offers a significant example of the relevance of varying degrees of ontological friction in social contexts.

We are now ready to formulate a qualitative sort of equation, which will be needed to analyze the relation between digital ICTs and informational privacy. 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 (imagine three of our students living in a tent during a holiday, while the fourth is left home alone) or in the agents (e.g., two of our students change their behaviour because the other two have quarrelled).

Because of their "data superconductivity", ICTs are well-known for being among the most influential factors that affect the ontological friction in the infosphere.[5] A crucial difference between old and new ICTs is *how* they affect it.

Ontological friction and the difference between old and new ICTs

In the past, ICTs have always tended to reduce what agents considered the normal degree of ontological friction in their environment. This already held true for the invention of the alphabet or the diffusion of printing. Photography and the rise of the daily press were no exceptions. One can easily sympathize with nineteenth century concerns about the impact on individuals' informational privacy of "[r]ecent inventions and business methods [...], [i]nstantaneous photographs and newspaper enterprise [...] and numerous mechanical devices" (Warren and Brandeis, 1890).

All this does not mean that, throughout history, informational privacy has constantly decreased in relation to the invention and spreading of ever more powerful ICTs. This would be a simplistic and mistaken inference. As emphasized above, changes in the nature both of the environment and of the agents play a pivotal role as well, so the actual ontological friction, and hence the corresponding degree of informational privacy in a region of the infosphere, are the result of a fine balance among several factors. Most notably, during the nineteenth and the twentieth centuries, following the industrial revolution, the social phenomenon of the new metropolis counteracted the effects of the latest ICTs, as urban environments fostered a type of informational privacy based on *anonymity*.[6] This is the sort of privacy enjoyed by a leaf in the forest, still inconceivable nowadays in rural settings or small villages. In the same period in which Warren and Brandeis were working on their classic article, the Edinburgh of Dr. Jekyll[7] and the London of Sherlock Holmes[8] already provided increasing opportunities for informational privacy through anonymity, despite the recent availability of new technologies.

Old ICTs have always tended to reduce the ontological friction in the infosphere because they *enhance* or *augment* the agents embedded in it. To understand why, consider the appliances available in our students' house.

Some appliances – e.g. a drill, a vacuum cleaner or a food mixer – are tools that *enhance* their users, exactly like an artificial limb. Tele-ICTs (e.g. the telescope, the telegraph, the radio, the telephone or the television) are enhancing in this sense. Some other appliances – e.g. a dishwasher, a washing machine or a refrigerator – are robots that *augment* their users insofar as well-specified tasks can be delegated to them, at least partially. Recording ICTs (e.g. the alphabet and the various writing and printing

[5] For a similar point see Moor (1997), who writes "When information is computerized, it is *greased* to slide easily and quickly to many ports of call" (p. 27).

[6] Anonymity is defined here as the unavailability of personal information, or the "noncoordinability of traits in a given respect", according to Wallace (1999).

[7] Stevenson's *The Strange Case of Dr Jekyll and Mr Hyde* was first published in 1886.

[8] Doyle's *A Study in Scarlet* was first published in 1887.

technologies, the tape or video recorder) are augmenting in this sense.

Enhancing and augmenting ICTs have converged and become bundled together. The Watergate scandal and Nixon's resignation would have been impossible without them. But whether kept separate or packaged together, old ICTs have always shared the fundamental feature of facilitating the information flow in the infosphere by increasingly empowering the agents embedded in it. This "agent-oriented" trend in old, predigital[9] ICTs is well represented by dystopian views of informationally omnipotent agents, able to overcome any ontological friction, to control every aspect of the information flow, to acquire any personal data and hence to implement the ultimate surveillance system, thus destroying all informational privacy, "the dearest of our possessions".

Now, according to a "continuist" interpretation of technological changes, digital ICTs should be treated as just one more instance of well-known, enhancing or augmenting ICTs. But then – the reasoning goes – if there is no radical difference between old and new (i.e. digital) ICTs, it is reasonable to argue that the latter cause increasing problems for informational privacy merely because they are orders of magnitude more powerful than past technologies in enhancing or augmenting agents in the infosphere. All past ICTs have tended to reduce the ontological friction in the infosphere by enhancing or augmenting the agents inhabiting it, but digital ICTs are no exception, so the 2P2Q explanation is correct. Orwell's "Big Brother" is readily associated with the ultimate database.

Although the continuist 2P2Q hypothesis is reasonable and intuitive, it overlooks the essence of the problem. In theory, ontological friction can both be reduced and increased. We have seen how the emergence of the urban environment actually produced more anonymity, and hence more ontological friction and more informational privacy. The difference between old and new ICTs is that the former tended to reduce informational privacy, whereas the latter can also increase it. This is because the former tended to enhance or augment the agents involved more and more, whereas the latter can also change the very nature of the infosphere (that is, of the environment itself, of the agents embedded in it and of their interactions). The 2P2Q explanation misses a fundamental difference between old and new ICTs: the former are enhancing or augmenting whereas the latter are best understood as re-ontologizing technologies, an important distinction that needs to be analyzed in some detail.

Digital ICTs as re-ontologizing technologies

Our model and a bit of science fiction will help to introduce the new concept of *re-ontologization*.[10]

Suppose that all the walls and the furniture in our students' house are transformed into perfectly transparent glass. Assuming our students have good sight, this will drastically reduce the ontological friction in the system. Imagine next that the students are transformed into proficient mind-readers and telepathists. Any informational privacy in this sort of Bentham's *PanOpticon* will become virtually impossible. The thought experiment illustrates how radical modifications in the very nature (a re-ontologization) of the infosphere can dramatically change the conditions of possibility of informational privacy.

The influence exercised by the new digital ICTs on the infosphere can now be analyzed in terms of its re-ontologization. Schematically, one can distinguish five fundamental trends.

1. *The digitization of the informational environment*. This is the most obvious way in which the new ICTs have re-ontologized the infosphere. The transition from analogue to digital data is very familiar and requires no explanation, but perhaps a brief comment may not go amiss. In their second study on information storage and flows, Lyman and Varian (2003) write that "Print, film, magnetic, and optical storage media produced about 5 exabytes of new information in 2002. Ninety-two percent of the new information was stored on magnetic media, mostly in hard disks. [...] Five exabytes of information is equivalent in size to the information contained in 37,000 new libraries the size of the Library of Congress book collections" (Lyman and Varian, 2003). Although the production of analogue data is still increasing, the infosphere is fast becoming progressively more digital.

2. *The homogenization of the processor and the processed*. The re-ontologization of the infosphere has also been caused by the fundamental convergence between digital resources and digital tools. The ontology of the information technologies available (e.g. software, databases, communication protocols etc.) is now the same as (and hence fully compatible with) the ontology of their objects. This was one of Turing's most consequential intuitions: in the re-ontologized infosphere, there is no longer any substantial difference between the processor and the processed and the digital deals effortlessly and seamlessly with the digital. This potentially eliminates one of the most long-standing bottlenecks in the infosphere, a major source of ontological friction.

[9] Orwell's *1984*, first published in 1949, contains no reference to computers or digital machines.

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

The increasing computerization of artefacts (from the cash machine to the fridge, from the car to the building, from one's underwear to a book, cf. the current debate on privacy and RFID[11]) and of whole social environments (the phenomenon of "Ubiquitous Computing" or "Ambient Intelligence"[12]) reminds us that soon it will be difficult to understand what life was in predigital times.

3. *The evolution of new informational agents*. This change concerns the emergence of artificial and hybrid agents (i.e. partly artificial and partly human; consider the group of our students as a single agent, equipped with digital cameras, laptops, palm pilots, mobiles, a wireless network, digital TVs, DVDs, CD players, etc.). These new artificial agents share the same ontology with their environment and can operate in it with much more freedom and control. This is where digital ICTs can be mistaken for mere *augmenting* technologies. Arguably, the infosphere will be progressively populated by artificial or hybrid agents, to which other (not necessarily human) agents will be able to delegate tasks and decisions. It is to be expected that the moral status of such agents will become an ever more challenging issue.[13]

4. *The informationalization of interactions*. In the re-ontologized infosphere populated by ontologically-equal entities and agents, where there is no ontological difference between processors and processed, interactions become equally digital. They are all interpretable as "read/write" (i.e., access/alter) activities, with "execute" the remaining type of process.

5. *The mutation of old agents into informational agents*. Finally, by re-ontologizing the infosphere, digital ICTs have also brought to light the intrinsically informational nature of human agents. This is not equivalent to saying that our students in the house have digital alter egos, some Messrs Hydes represented by their @s, blogs and https. This trivial point only encourages us to mistake digital ICTs for merely *enhancing* technologies. The informational nature of agents should not be confused with a "data shadow"[14] either. The more radical change, brought about by the re-ontologization of the infosphere, has been the disclosure of human agents as informational entities among other informational entities, in the following sense.

Recall the distinction between enhancing and augmenting appliances. The switches and dials of the former are interfaces meant to plug in the appliance to the user's body ergonomically. The data and control panels of augmenting appliances are instead interfaces between different possible worlds: on the one hand there is the human user's *Umwelt*,[15] and on the other hand there are the dynamic, watery, soapy, hot and dark world of the dishwasher; the equally watery, soapy, hot and dark but also spinning world of the washing machine; or the still, aseptic, soapless, cold and potentially luminous world of the refrigerator. These robots can be successful because they have their environments "wrapped" and tailored around their capacities, not vice versa. Imagine our students trying to build a droid like C3PO capable of washing their dishes in the sink exactly in the same way as they would.

Computers and digital ICTs are not augmenting or empowering in the sense just explained. They are ontologizing devices because they engineer environments that the user is then enabled to enter through (possibly friendly) gateways. So, whilst a dishwasher interface is a panel through which the machine enters into the user's world, a computer interface is a gate through which a user can be telepresent in the infosphere (Floridi, forthcoming-b). This simple but fundamental difference underlies the many spatial metaphors of "cyberspace", "virtual reality", "being online", "surfing the web", "gateway" and so forth.

The re-ontologization of the infosphere, just sketched, has been causing an epochal, unprecedented migration of humanity from its *Umwelt* to the infosphere itself. Inside it, humans are informational agents among other informational (possibly artificial) agents. They operate in an environment that is friendlier to "digital creatures". They have the ontological status of informational entities. And as digital immigrants are replaced by digital natives, the latter may come to appreciate that there is no ontological difference between infosphere and *Umwelt*, only a difference of levels of abstractions (Floridi and Sanders, 2004a; forthcoming).

Informational privacy in the re-ontologized infosphere

To summarize, so far it has been argued that informational privacy is a function of the ontological friction in the infosphere. Many factors can affect the

[11] Radio Frequency IDentification, a method of storing and remotely retrieving data using tags or transponders.

[12] Coroama et al. (2004), Bohn et al. (2004) and Brey (2005) offer an ethical evaluation of privacy-related issues in Ambient Intelligence environments. For a technically informative and balanced assessment see also Gow (2005).

[13] The issue of artificial morality is analyzed in Floridi and Sanders (2004b).

[14] The term is introduced by Westin (1968) to describe a digital profile generated from data concerning a user's habits online.

[15] The outer world, or reality, as it affects the agent inhabiting it.

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 most significantly by re-ontologizing it; therefore, 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.

Framing the revolutionary nature of digital ICTs in this ontological way offers several advantages. The first can be highlighted immediately: the ontological hypothesis is perfectly consistent with the 2P2Q hypothesis, since the re-ontologization of the infosphere explains why digital ICTs are so successful, in terms of the quantity, quality and speed at which they can variously process their data. It follows that the ontological hypothesis can inherit whatever explanatory benefits are carried by the 2P2Q hypothesis.

Four other advantages can be listed here but each of them requires a more detailed analysis: (1) contrary to the 2P2Q hypothesis, the new approach explains why digital ICTs can also enhance informational privacy, although (2) there is still a sense in which the information society provides less protection for informational privacy than the industrial society did. Above all, (3) the ontological hypothesis provides the right frame within which to assess contemporary interpretations of informational privacy and (4) can indicate how we might wish to proceed in the future in order to protect informational privacy in the newly re-ontologized infosphere. Let us consider each point in turn.

Empowering the informational agent

In the re-ontologized infosphere, any informational agent has an increased power not only to gather and process personal data, but also to control and protect them. Recall that the digital now deals with the digital effortlessly. The phenomenon cuts both ways. It has led not only to a huge expansion in the flow of personal information being recorded, processed and exploited, but also to a large increase in the types and levels of control that agents can exercise on their personal data. And while there is only a certain amount of personal data that an agent may care to protect, the potential growth of digital means and measures to control their life-cycle does not seem to have a foreseeable limit. If privacy is the right of individuals (being these single persons, groups, or institutions) to control the life-cycle (especially the generation, access, recording and usage) of their information and determine for themselves when, how, and to what extent their information is processed by others, then one must agree that digital ICTs may enhance as well as hinder the possibility of enforcing such right.

At their point of generation, digital ICTs can foster the protection of personal data, e.g. by means of encryption, anonymization, password-encoding, firewalling, specifically devised protocols or services, and, in the case of externally captured data, warning systems.

At their point of storage, legislation, such as the Data Protection Directive passed by the EU in 1995, guarantees that no ontological friction, already removed by digital ICTs, is surreptitiously reintroduced to prevent agents from coming to know about the existence of personal data records, and from accessing them, checking their accuracy, correcting or upgrading them or demanding their erasure.

And at their point of exploitation – especially through data-mining, -sharing, -matching and -merging – digital ICTs could help agents to control and regulate the usage of their data by facilitating the identification and regulation of the relevant users involved.

At each of these three stages, solutions to the problem of protecting informational privacy can be not only self-regulatory and legislative but also technological, not least because informational privacy infringements can more easily be identified and redressed also thanks to digital ICTs.

All this is not to say that we are inevitably moving towards an idyllic scenario in which our PETs (Privacy Enhancing Technologies) will fully protect our private lives and information against harmful PITs (Privacy Intruding Technologies). Such optimism is unjustified. But it does mean that digital ICTs can already provide some means to counterbalance the risks and challenges that they represent for informational privacy, and hence that no fatalistic pessimism is justified either. Digital ICTs do not necessarily erode informational privacy; they can also enhance and protect it. A good example is provided by the P3P (Platform for Privacy Preferences) initiative of the W3C (World Wide Web Consortium, see http://www.w3.org/P3P/).

The return of the (digital) community

Because digital ICTs are radically modifying our informational environments, ourselves and our interactions, it would be naïve to expect that informational privacy in the future will mean exactly what it meant in the industrial Western world in the middle of the last century.

Previously, we saw that, between the end of the nineteenth and the beginning of the twentieth century, the ontological friction in the infosphere, actually reduced by old ICTs, was nevertheless increased by social conditions favouring anonymity and hence a new form of informational privacy. In this respect, the diffusion of digital ICTs has finally brought to completion the process begun with the invention of printing. We are back into the now digital community, where anonymity can no longer be taken for granted, and hence where the decrease in ontological friction caused by old and new ICTs can have all its full-blown effects on informational privacy. In Britain, for example, public places are constantly monitored by 1.5 m CCTV systems, with the result that the average citizen is recorded 300 times a day (*The Economist*, (Jan 23rd 2003). The digital ICTs that allowed terrorists to communicate undisturbed over the Internet were also responsible for the identification of the London bombers in a matter of hours (Figure 1). Likewise, mobile phones are increasingly useful as forensic evidence in trials. In Britain, cell site analysis (a form of triangulation that estimates the location of a mobile phone when it is used) helped disprove Ian Huntley's alibi and convict him for the murdering of Holly Wells and Jessica Chapman. Sherlock Holmes has the means to fight Mr. Hyde.

How serious and dangerous is it to live in a glassy infosphere? Human agents tend to be acquainted with different environments that have varying degrees of ontological friction and hence to be rather good at adapting themselves accordingly. As with other forms of fine equilibria, it is hard to identify, for all agents in any environments, a common, lowest threshold of ontological friction below which human life becomes increasingly unpleasant and ultimately unbearable. It is clear, however, that a particular threshold has been overcome when the agents are willing to employ resources, run risks or expend energy to restore it, e.g. by building a higher fence, by renouncing a desired service, or by investing time in revising a customer profile. On the other hand, different agents have different degrees of sensitivity. One needs to remember that several factors (character, culture, upbringing, past experiences etc.) make each agent a unique individual. To one person, a neighbour capable of seeing one's garbage in the garden may seem an unbearable breach of their privacy, which it is worth any expenditure and effort to restore; to another person, living in the same room with several other family members may feel entirely unproblematic. Human agents can adapt to very low levels of ontological friction. Virginia Woolf's essay on Montaigne discusses the lack of ontological friction that characterizes public figures in public contexts. Politicians

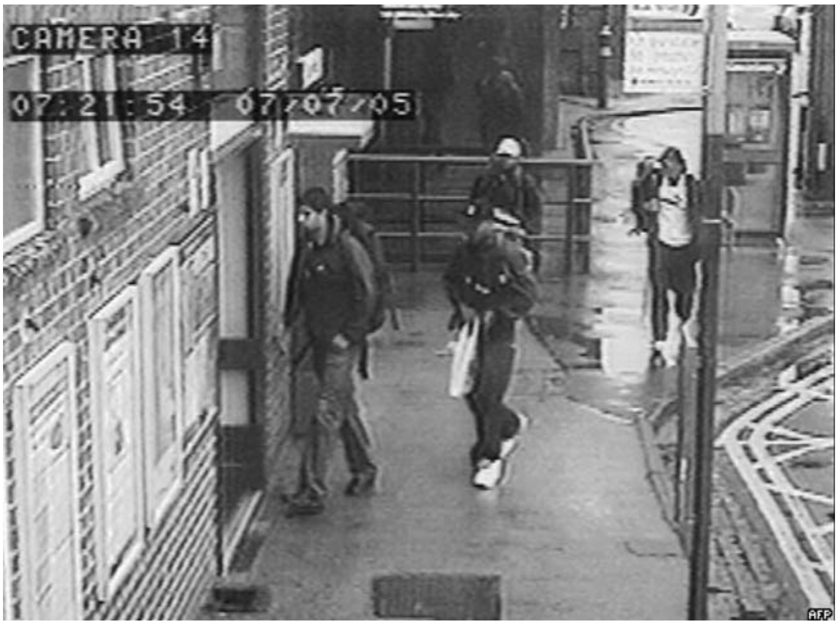

Figure 1. CCTV image of the four London terrorists as they set out from Luton.

and actors are used to environments were privacy is a rare commodity. Likewise, people involved in "Big Brother" (but "Truman Show" would be a more appropriate label) programmes show a remarkable capacity to adapt to settings where any ontological friction between them and the public is systematically reduced, apparently for the sake of entertainment. In far more tragic and realistic contexts, prisoners in concentration camps are subject to extreme duress due to both intended and unavoidable rarefaction of ontological friction (Levi, 1959).

The information society has revised the threshold of ontological friction and therefore provides a different sense in which its citizens appreciate their informational privacy. Your supermarket knows exactly what you like, but so did the owner of the grocery where your grandparents used to shop. Your bank has detailed records of all your visits and of your financial situation, but how exactly is this different from the old service? A phone company could analyze and transform the call data collected for billing purposes into a detailed subscriber profile: social network (names and addresses of colleagues friends or relatives called), possible nationality (types of international calls), times when one is likely to be at home and hence working patterns, financial profile (expenditure) and so forth. Put together the data from the supermarket, the bank and the phone company, and inferences of all sorts could be drawn for one's credit rating. Yet so they could be and were in Alexandre Dumas' *The Count of Monte Cristo* (1844). *Some* steps forward into the information society are really steps back into a small community and, admittedly, the claustrophobic atmosphere that may characterize it.

In the early stages in the history of the Web, roughly when Netscape was synonymous with browser, users believed that being online meant being entirely anonymous. A networked computer was like Gyges' ring in Plato's *Republic* (359b–360d): it made one invisible, unaccountable and therefore potentially less responsible, socially speaking. Turing would certainly have appreciated the (at the time) popular comic strip in which a dog, typing an email on a computer, confessed to another dog that "when you are on the Internet nobody can guess who you are". Nowadays, the strip is not funny anymore, only outdated. Cookies, monitoring software and malware (malicious software, such as spyware) have made people realize that the screen in front of them is not a shield for their privacy or Harry Potter's invisibility cloth, but a window on their lives online, through which virtually anything could be seen. They expect web sites to monitor and record their activities and do not even mind for what purpose. They accept that being online is one of the less private things in life.[16] The screen is a monitor and is monitoring you.

A few years ago, a journalist at *The Economist* ran an experiment (*The Economist*, December 16th 1999). He asked a private investigator, "Sam", to show what information it was possible to gather about someone. The journalist himself was to be the subject of the experiment. The country was Britain, the place where the journalist lived. The journalist provided Sam with only his first and last names. Sam was told not to use "any real skulduggery (surveillance, going through her domestic rubbish, phone-tapping, hacking, that sort of thing)". The conclusion? By using several databases and various ICTs, "Without even talking to anyone who knows me, Sam [...] had found out quite a bit about me. He had a reasonable idea of my personal finances – the value of my house, my salary and the amount outstanding on my mortgage. He knew my address, my phone number, my partner's name, a former partner's name, my mother's name and address, and the names of three other people who had lived in my house. He had 'found' my employer. He also had the names and addresses of four people who had been directors of a company with me. He knew my neighbours' names."

Shocking? Yes, in the anonymous industrial society, but not really in the pre-industrial village before it, or in the information society after it. In Guarcino, a small village south of Rome of roughly a thousand people, everybody knows everything about everybody else, "vita, morte e miracoli", "life, death and miracles", as they say in Italian. There is very little ontological friction provided by anonymity so there is very little informational privacy in that respect. A difference with the information society is that we have seen that the latter has the digital means to protect what the small village must necessarily forfeit.

There are of course many other dissimilarities. As Paul Oldfield has rightly stressed,[17] the comparison between today's information society and the small

[16] "The best long-term assessment of public attitudes toward privacy is provided by Columbia's Alan Westin, who has conducted a series of polls over the last thirty years on this issue. On average, he finds that one quarter of the American public cares deeply about keeping personal information secret, one quarter doesn't care much at all, and roughly half are in the middle, wanting to know more about the benefits, safeguards, and risks before providing information. Customer behaviour in the marketplace – where many people freely provide personal information in exchange for various offers and benefits – seems to bear out this conclusion" Walker (2000).

[17] Private communication. The rest of this section is largely based on comments sent to me by Paul Oldfield.

community of the past, where "everybody knows everything", must be taken with more than a pinch of salt. History may repeat itself, yet never too monotonously. Small communities had a high degree of intra-community transparency (like a shared house) but a low degree of inter-community transparency (they were not like the Big Brother house, visible to outside viewers). So in those communities, the breaches of privacy were reciprocal, yet there were few breaches of privacy across the boundary of the community. This is quite different from today's information society, where there can be very little transparency within the communities we live or work in (we hardly know our neighbours, and our fellow-workers have their privacy rigorously protected), yet data-miners, hackers and institutions can be very well informed about us. Breaches of privacy from outside are common. What is more, we do not even know whether they know our business. On the other hand, part of the value of this comparison lies in the size of the community taken into consideration. A special trait of the information society is precisely its lack of boundaries, its global nature. We live in a single infosphere, which has no "outside" and where intra- and inter-community relations are more difficult to distinguish. The types of invasion of privacy are quite different too. In the small community, breaches of privacy might shame or discredit you. Interestingly, Augustine usually speaks of privacy in relation to the topic of intercourse in married couples, and he always associates it to secrecy and secrecy to shame or embarrassment. Or they might disclose your real identity or character (more on this later). Things that were private became public knowledge. In the information society, such breaches involve unauthorized collection of information, not necessarily its publication. Things that are private may not become public at all; they may be just accessed and used by privileged others. The small community also had its own self-regulations for limiting breaches of privacy. Everyone knew that they were as subject to scrutiny as everyone else, and this set an unspoken limit on their enthusiasm for intruding into others' affairs.

Assessing theories of privacy

Once it is acknowledged that digital ICTs have re-ontologized the infosphere, it becomes easier to assess the available theories of informational privacy and its moral value.

Two theories are particularly popular: the *reductionist interpretation* and the *ownership-based interpretation.*

The reductionist interpretation argues that the value of informational privacy rests on a variety of undesirable consequences that may be caused by its breach, either personally (e.g. distress) or socially (e.g. unfairness). Informational privacy is a utility, also in the sense of providing an essential condition of possibility of good human interactions, e.g. by preserving human dignity or by providing political checks and balances.

The ownership-based interpretation argues that informational privacy needs to be respected because of each person's rights to bodily security and property (where "property of x" is classically understood as the right to exclusive use of x). A person is said to *own* his or her information (information about him- or herself) – recall Virginia Woolf's "infinitely the dearest of our possessions" – and therefore to be entitled to control its whole life-cycle, from generation to erasure.[18]

The two approaches are not incompatible, but they stress different aspects of informational privacy. One is more oriented towards a consequentialist assessment of privacy protection or violation. The other is more oriented towards a "natural rights" understanding of the concept of privacy itself, in terms of private or intellectual property. Unsurprisingly, they both compare privacy breach to a trespass[19] or unauthorized invasion of, or intrusion in, a space or sphere of personal information, whose accessibility and usage ought to be fully controlled by its owner and hence kept private. A typical example is provided by the border-crossing model of informational privacy developed by Gary T. Marx since the late nineties (see now Marx, 2005).

The reductionist interpretation is not entirely satisfactory. Defending the need for respect for informational privacy in view of the potential misuse of the information acquired is certainly reasonable, especially from a consequentialist perspective, but it may be inconsistent with pursuing and furthering social interests and welfare. For, although it is obvious that even some public personal information may need to be protected – e.g. against profiling or unrestrained electronic surveillance – it remains unclear, on a purely reductionist basis, whether a society devoid of any informational privacy may not be a

[18] The debate on the ownership-based interpretation developed in the seventies, see Scanlon (1975) and Rachels (1975), who criticize Thomson (1975), who supported an interpretation of the right to privacy as being based on property rights.

[19] See Spinello (2005) for a recent assessment of the use of the trespassing analogy in computer-ethical and legal contexts. Charles Ess has pointed out to me that comparative studies have shown such spatial metaphors to be popular only in Western contexts.

better society, with a higher, common welfare.[20] It has been argued, for example, that the defence of informational privacy in the home may actually be used as a subterfuge to hide the dark side of privacy: domestic abuse, neglect or mistreatment. Precisely because of reductionist-only considerations, even in democratic societies such as the UK and the US, it tends to be acknowledged that the right to informational privacy can be overridden when other concerns and priorities, including business needs, public safety and national security, become more pressing. All this is despite the fact that article 12 of *The Universal Declaration of Human Rights* clearly indicates 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."

The ownership-based interpretation also falls short of being entirely satisfactory. Three problems are worth highlighting here:

(i) the issue of informational contamination undermining passive informational privacy; this is the unwilling acquisition of information or data (e.g. mere noise) imposed on someone by some external source. Brainwashing may not occur often, but junkmail, or the case of a person chatting loudly on a mobile near us, are unfortunately very common experiences of passive privacy breach, yet no informational ownership seems to be violated;

(ii) the issue of informational privacy in public contexts; informational privacy is often exercised in public spaces, that is, in spaces which are not only socially and physically public – a street, a car park, a pub – but also informationally public – anyone can see the newspaper one buys, the bus one takes, the T-shirt one wears, the drink one is ordering (Patton, 2000). How could a CCTV system be a breach of someone's privacy if the agent is accessing a space which is public in all possible senses anyway? and

(iii) the metaphorical and imprecise use of the concept of "information ownership", which cannot quite explain the lossless acquisition (or usage) of information: contrary to other things that one owns, one's personal information is not lost when acquired by someone else. Analyses of privacy based on "ownership" of an "informational space" are metaphorical twice over.

The ontological interpretation of informational privacy and its value

Both the reductionist and the ownership-based interpretation fail to acknowledge the radical change brought about by digital ICTs. They belong to an industrial culture of material goods and of manufacturing/trading relations. They are overstretched when trying to cope with the new challenges offered by an informational culture of services and usability.

Warren and Brandeis (1890) had already realized this limit very insightfully: "where the value of the production [of some information] is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, *it is difficult to regard the right as one of property, in the common acceptation of the term*" (p. 25, emphasis added).

More than a century later, 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 informational social agents.

Such re-interpretation is achieved by considering each person 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.

The following passage by Marcel Proust, though admittedly referring to the social construction of the individual, helps to conveys the idea of a person as an informational entity: "But then, even in the most insignificant details of our daily life, none of us can be said to constitute a material whole, which is identical for everyone, and need only be turned up like a page in an account-book or the record of a will; our social personality is created by the thoughts of other people. Even the simple act which we describe as "seeing some one we know" is, to some extent, an intellectual process. We pack the physical outline of the creature we see with all the ideas we have already formed about him, and in the complete picture of him which we compose in our minds those ideas have certainly the principal place. In the end they come to fill out so completely the curve of his checks, to follow so exactly the line of his nose, they blend so harmoniously in the sound of his voice that these seem to be no more than a transparent envelope, so that each time we see the

[20] Moor (1997) infers from this that informational privacy is not a core value, i.e. a value that "all normal humans and cultures need for survival", but then other values he lists as "core" are not really so in his sense, e.g. happiness and freedom. According to Moor, privacy is also intrinsically valuable, while being the expression of the core value represented by security.

face or hear the voice it is our own ideas of him which we recognize and to which we listen." (*Remembrance of Things Past – Swann's Way*).

The ontological 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 needs 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 reductionists – recall the example of the glassy house and of our mentally super-enhanced students – 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.

The advantage of the ontological interpretation over the reductionist one is then that consequentialist concerns may override respect for informational privacy, whereas the ontological interpretation, by equating its protection to the protection of personal identity, considers it a fundamental and inalienable right,[21] so that, by default, the presumption should always be in favour of its respect. As we shall see, this is not to say that informational privacy is never negotiable in any degree.

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 cloning and breeding someone'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.[22] The first difficulty facing the ownership-based interpretation is thus avoided: in either case, the ontological interpretation suggests that there is no difference between one's informational sphere and one's personal identity. "You are your information", so anything done to your information is done to you, not to your belongings. The 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.

Heuristically, violations of informational privacy are now more fruitfully compared to a digital 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. It is a *Doppelgänger*, as Richard Avedon described it once, when speaking of his photograph of Henry Kissinger ("Is it just a shadow representation of a man? Or is it closer to a doppelgänger, a likeness with its own life, an inexact twin whose afterlife may overcome and replace the original?"). A further advantage, in this change of 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. The second problem affecting the ownership-based interpretation is also solved.

As for the third problem, one may still argue that an agent "owns" his or her information, yet no longer in the metaphorical sense seen above, 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 *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. It is worth quoting Warren and Brandeis (1890) once again: ""[...] the protection afforded to thoughts, sentiments, and emotions [...] is merely an instance of the enforcement of the more general right

[21] For a different view see Volkman, 2003.

[22] This view is close to the interpretation of privacy in terms of protection of human dignity defended by Bloustein (1964).

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)".

This ontological conception has started being appreciated by more advanced information societies where identity theft is the fastest growing white-collar offence, as Figure 2 well indicates. Informational privacy is the other side of identity theft, to the point that, ironically, for every person whose identity has been stolen (around 10m Americans are victims annually) there is another person (the thief) whose identity has been "enhanced".

Recent problems affecting Google and its privacy policy convey a similar picture. As Kevin Bankston, staff attorney at the Electronic Frontier Foundation, remarks "Your search history shows your associations, beliefs, perhaps your medical problems. *The things you Google for define you.* [...] data that's practically a printout of what's going on in your brain: What you are thinking of buying, who you talk to, what you talk about" (quoted in Mills, 2005, emphasis added).

As anticipated, the ontological interpretation reshapes some of the assumptions behind our still "industrial" conception of informational privacy. Three examples are indicative of this transition.

If personal information is finally acknowledged to be a constitutive part of someone's personal identity and individuality, then one day it may become strictly illegal to trade in some kinds of personal information, exactly as it is illegal to trade in human organs (including one's own) or slaves. The problem of child pornography may also be revisited in light of an ontological interpretation of informational privacy. At the same time, one might relax one's attitude towards some kinds of "dead personal information" that, like "dead pieces of oneself", are not really or no longer constitutive of oneself. One should not sell one's kidney, but can certainly sell one's hair or be rewarded for giving blood. Recall the experiment of the journalist at *The Economist*. Very little of what Sam had discovered could be considered ontologically constitutive of the person in question. We are constantly leaving behind a trail of personal data, pretty much in the same sense in which we are losing a huge trail of dead cells. The fact that nowadays digital ICTs allow our data trails to be recorded, monitored, processed and used for social, political or

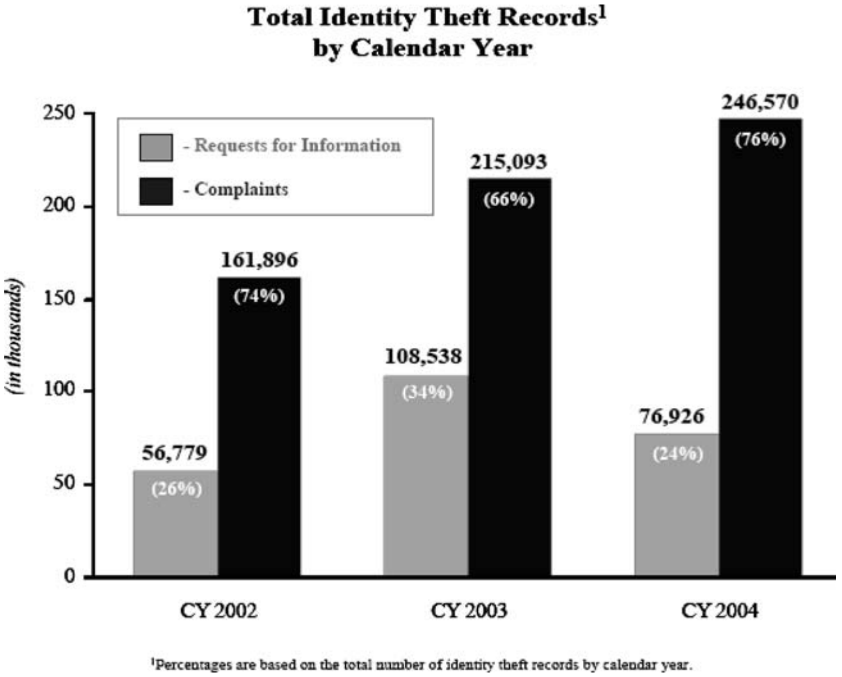

Figure 2. Identity thefts in the US between 2002 and 2004. Source: Data from Consumer Sentinel and the Identity Theft Data Clearinghouse, National and State Trends in Fraud & Identity Theft, January–December 2004. Federal Trade Commission, February 1, 2005.

commercial purposes is a strong reminder of our informational nature as individuals and might be seen as a new level of ecologism, as an increase in what is recycled and a decrease in what is wasted.

At the moment, all this is just speculation and in the future it will probably be a matter of fine adjustments of ethical sensibilities, but the third Geneva Convention (1949) already provides a clear test of what might be considered "dead personal information": a prisoner of war need only give his or her name, rank, date of birth, and serial number and no form of coercion may be inflicted on him or her to secure any further information, of any kind. If we were all considered "prisoners of the information society", our informational privacy would be well protected and yet there would still be some personal data that would be perfectly fine to share with any other agent, even hostile ones.

A further issue that might be illuminated by the ontological interpretation is that of confidentiality. The sharing of private information with someone, implicitly or explicitly, is based on a relation of profound trust that joins together the agents involved. This coupling is achieved by allowing the agents to be partly constituted, ontologically, by the same information. Visually, the informational identities of the agents involved now overlap, at least partially, as in a Venn diagram. The union of the agents forms a single unity, a supra-agent. Precisely because entering into a new supra-agent is a delicate and risky operation, care should be exercised before "melding" oneself with other individuals by sharing personal information or its source i.e. common experiences. Confidentiality is a bond that is hard and slow to forge properly, yet resilient to many external forces when finally in place, as the supra-agent is stronger than the constitutive agents themselves. Relatives, friends, classmates, fellows, colleagues, comrades, companions, partners, team-mates, spouses and so forth may all have experienced the nature of such a bond, the stronger taste of a "we". But it is also a bond very brittle and difficult to restore when it comes to betrayal, since the disclosure, deliberate or unintentional, of some personal information in violation of confidence can entirely and irrecoverably destroy the privacy of the new, supra-agent born out of the joining agents, by painfully tearing them apart. We shall return to the topic of trust and confidentiality at the end of this article.

A third and final issue can be touched upon rather briefly, as it was already mentioned above: 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.[23]

Informational privacy, personal identity and biometrics

On September 12, 1560 the young Montaigne attended the public trial of Arnaud du Tilh, an impostor who was sentenced to death for having faked his identity. Many acquaintances and family members, including the wife Bertrande, had been convinced for a long while that he was Martin Guerre, returned home after many years of absence. Only when the real Martin Guerre came home was Arnaud's actual identity finally ascertained.

Had Martin Guerre always been able to protect his personal information, Arnaud du Tilh would have been unable to steal his identity. Clearly, the more one's informational privacy is protected the more one's personal identity can be safeguarded. This new qualitative equation is a direct consequence of the ontological interpretation. Personal identity also depends on informational privacy. The difficulty facing our contemporary society is how to combine the new equation with the other equation, introduced above, according to which informational privacy is a function of the ontological friction in the infosphere. Ideally, one would like to reap all the benefits from

(a) the highest level of information flow; and hence from
(b) the lowest level of ontological friction; while enjoying
(c) the highest level of informational privacy protection; and hence
(d) the highest level of personal identity protection.

The problem is that (a) and (d) seem incompatible: facilitate and increase the information flow through digital ICTs and the protection of one's personal identity is bound to come under increasing pressure. You cannot have an identity without having an identikit. Or so it seems, until one realizes that the information flowing in (a) consists of all sorts of data, including *arbitrary* data *about* oneself (e.g. a name and surname) that are actually shareable, whereas the

[23] 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.

information required to protect (d) can be *ontic* data, that is, data *constituting* someone (e.g. someone's DNA) that are hardly sharable by nature.[24] Enter biometrics.

Personal identity is the weakest link and most delicate element in our problem. Even nowadays, personal identity is regularly protected and authenticated by means of some *arbitrary* data, *randomly* or *conventionally* attached to the bearer/user, like a mere label: a name, an address, a Social Security number, a bank account, a credit card number, a driving licence number, a PIN and so forth. Each label in the list has no ontologically constitutive link with its bearer; it is merely associated with someone's identity and can easily be detached from it without affecting it. The rest is a mere consequence of this "detachability". The more the ontological friction in the infosphere decreases, the swifter these detached labels can flow around, and the easier it becomes to grab and steal them and use them for illegal purposes. Arnaud du Tilh had stolen a name and a profile and succeeded in impersonating Martin Guerre for many years in a rather small village, within a community that knew him well, fooling even Martin's wife, apparently. Eliminate all personal interactions and identity theft becomes the easiest thing in the world.

A quick and dirty way to fix the problem would be to clog the infosphere by slowing down the information flow. Building some traffic calming device, as it were. It seems the sort of policy popular among some IT officers and bank managers, keen on not allowing this or that operation for security reasons, for example. However, as with all counter-revolutionary or anti-historical approaches, "resistance is futile": trying to withstand the evolution of the infosphere only harms current users and, in the long run, fails to deliver an effective solution.

A much better approach is to ensure that the ontological friction keeps decreasing, thus benefiting all the inhabitants of the infosphere, while safeguarding personal identity by data that are not arbitrary labels about, but rather constitutive traits of, the person in question. Arnaud du Tilh and Martin Guerre looked very similar, yet this was as far as biometrics went in the sixteenth century. Today, biometric digital ICTs are increasingly used to authenticate a person's identity by measuring the person's physiological traits – such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements or DNA sampling – or behavioral features, such as typing patterns. Since they also require the person to be identified to be physically present at the point-of-identification, biometric systems provide a very reliable way of ensuring that the person is who the person claims to be; of course not always, and not infallibly – after all Montaigne used the extraordinary case of Martin Guerre to challenge human attempts ever to reach total certainty – but far more successfully than any arbitrary label can. It is a matter of degree.

All this is not to say that we should embrace biometrics as an unproblematic panacea. As Alterman (2003) has correctly shown, there are many risks and limits in the use of such technologies as well. But it is significant that digital ICTs, in their transformation of the information society into a digital community, are partly restoring, partly improving (see the case of Martin Guerre) that reliance on personal acquaintance that characterized relations of trust in any small town. By giving away some information, one can safeguard one's identity and hence one's informational privacy, while taking advantage of interactions that are personalized (through preferences derived from one's habits and behaviours) and customized (through preferences derived from one's expressed choices). In the digital community, you are a recognized individual, whose tastes, inclinations, habits, preferences etc. are known to the other agents, who can adapt their behaviour accordingly.

As for protecting the privacy of biometric data, again, no rosy picture should be painted, but if one applies the "Convention of Geneva" test, it seems that even the worst enemy could be allowed to authenticate someone's identity by measuring her fingerprints or his eye retinas. They seem to be personal data that is worth sacrificing in favour of the extra protection they can offer of one's personal identity and private life.

Once a cost/benefit analysis is taken into account, it makes sense to rely on authentication systems that do not lend themselves so easily to misuse. In the digital community, one is one's own information and can be (biometrically) recognized as oneself as one was in the small village. The case of Martin Guerre is there to remind us that mistakes are still possible. But their likelihood decreases dramatically the more biometric data one is willing to check. On this, Penelope can teach us a final lesson.

Conclusion

When Odysseus returns to Ithaca, he is identified four times. Argos, his old dog, is not fooled and recognizes him despite his disguise as a beggar. Then Eurycleia, his wet-nurse, while bathing him, recog-

[24] On the tripartite distinction between information as, about or for reality see Floridi (2004).

nizes him by a scar on his leg, which he had received from a boar when hunting. He then proves to be the only man capable of stringing Odysseus' bow. All these are biometric tests no Arnaud du Tilh would have passed. But then, Penelope is no Bertrande either. She does not rely on any "unique identifier" but finally tests Odysseus by asking Eurycleia to move the bed in their wedding-chamber. Odysseus protests that this is impossible: he himself had built the bed around a living olive tree, which is now one of its legs. This is a crucial piece of information that only Penelope and Odysseus ever shared. By naturally relying on it, Odysseus restores Penelope's full trust. She recognizes him as the real Odysseus not because of who he is or how he looks, but, ontologically, because of the information that they have in common and that constitutes both of them as a couple. Through the sharing of this piece of information, identity is restored and the supra-agent is reunited. There is a line of continuity between the roots of the olive tree and the married couple. For Homer, their bond was *homophrosyne* (like-mindedness); to Shakespeare, it was the marriage of true minds. To us, it is informational privacy that admits no ontological friction.

Acknowledgements

Previous versions of this paper were presented at the seminar *Bridging Cultures: Computer Ethics, Culture, and ICT* (NTNU, Trondheim, 6 June, 2005) and at the *Sixth International Conference of Computer Ethics: Philosophical Enquiry* (CEPE2005, University of Twente, 18 July, 2005). I wish to thank all the participants and especially Phil Brey, Charles Ess, Johnny Søraker, Bernd Carsten Stahl and May Thorseth and the anonymous referees of the journal for their comments. Paul Oldfield and Matteo Turilli read a final version and suggested several crucial improvements. None of them is responsible for any of its shortcomings.

References

A. Alterman. A Piece of Yourself: Ethical Issues in Biometric Identification. *Ethics and Information Technology*, 5(3): 139–150, 2003.

F. Becker and W. Sims, *Offices That Work: Balancing Cost, Flexibility, and Communication*. Cornell University International Workplace Studies Program, New York, 2000.

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

J. Bohn, V. Coroama, M. Langheinrich, F. Mattern and M. Rohs. Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. *Journal of Human and Ecological Risk Assessment*, 10(5): 763–786, 2004.

P. Brey. Freedom and Privacy in Ambient Intelligence. In Philip Brey, Frances Grodzinsky, and Lucas Introna, editors, *Ethics of New Information Technology – Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry (Cepe2005)*, pp. 91–100. Enschende, CEPTES University of Twente, 2005.

T.W. Bynum and S. Rogerson, *Computer Ethics and Professional Responsibility*. Blackwell, Oxford, 2004.

V. Coroama, J. Bohn and F. Mattern. Living in a Smart Environment – Implications for the Coming Ubiquitous Information Society, *IEEE SMC 2004, The Hague, The Netherlands, October 10–13*, pp. 5633–5638, 2004.

L. Floridi. Information Ethics: On the Philosophical Foundations of Computer Ethics. *Ethics and Information Technology*, 1(1): 37–56, 1999. Reprinted, with some modifications, in *The Ethicomp Journal*, 1(1), 2004, http://www.ccsr.cse.dmu.ac.uk/journal/articles/floridi_1_philosophical.pdf.

L. Floridi. Information. In L. Floridi, editor, *The Blackwell Guide to the Philosophy of Computing and Information*, pp. 40–61. Blackwell, Oxford, New York, 2004.

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

L. Floridi. Presence: From Epistemic Failure to Successful Observability. *Presence: Teleoperators and Virtual Environments*, Forthcoming-b.

L. Floridi and J.W. Sanders. The Method of Abstraction. In M. Negrotti, editor, *Yearbook of the Artificial. Nature, Culture and Technology. Models in Contemporary Sciences*, pp. 177–220. Peter Lang, Bern, 2004a.

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

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.

L. Floridi and J.W. Sanders. Levellism and the Method of Abstraction, Forthcoming. The final draft of this paper is available as IEG – Research Report 22.11.04, see http://www.wolfson.ox.ac.uk/~floridi/pdf/latmoa.pdf.

A.M. Froomkin. The Death of Privacy?. *Stanford Law Review*, 52: 1461–1543, 2000.

S. Garfinkel, *Database Nation : The Death of Privacy in the 21st Century*. O'Reilly, Beijing, Cambridge, 2000.

G. Gow. *Consumers and Privacy in Ubiquitous Network Societies – Background Paper*, 2005. http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf retrieved on 16th of August 2005.

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

P. Levi, *If This Is a Man*. Orion Press, London, 1959.

P. Lyman and H.R. Varian. How Much Information? 2003, http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm#summary, retrieved on 16th of August 2005.

G.T. Marx. Some Conceptual Issues in the Study of Borders and Surveillance. In Elia Zureik and M.B. Salter, editors, *Global Surveillance and Policing – Borders, Security, Identity*. Willan Publishing, Cullompton, Devon, 2005, chapter 2.

E. Mills. Google Balances Privacy, Reach. *C|Net News.com*. 2005, http://news.com.com/Google + balances + privacy%2C + reach/2100-1032_3-5787483.html retrieved on 30th of August 2005.

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

J.W. Patton. Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places. *Ethics and Information Technology*, 2(3): 181–187, 2000.

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

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

R.A. Spinello. Trespass and Kyosei in Cyberspace. In R.A. Spinello and H.T. Tavani, editors, *Intellectual Property Rights in a Networked World: Theory and Practice*. Idea Group Inc., Hershey, PA, 2005, chapter 8.

H.T. Tavani, *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. John Wiley & Sons, New York, 2003.

The Economist December 2nd 2004 Your Cheating Phone.

The Economist December 16th 1999, Living in the Global Goldfish Bowl.

The Economist Jan 23rd 2003, SURVEY: THE INTERNET SOCIETY.

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

A.M. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2(42): 230–265, 1936.

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

K. Walker. Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange. *Stanford Technology Law Review*, 2: 1–50, 2000.

K.A. Wallace. Anonymity. *Ethics and Information Technology*, 1(1): 23–35, 1999.

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

A.F. Westin, *Privacy and Freedom 1st*. Atheneum, New York, 1968.