Special issue: Digitize and transfer

Numéro spécial: Numériser et transmettre

SSI

Jean-Gabriel Ganascia

The generalized sousveillance society

Abstract. *This article is based on the notion of 'sousveillance', which was invented by Steve Mann to describe the present state of modern technological societies where anybody may take photos or videos of any person or event, and then diffuse the information freely all over the world. The article shows how sousveillance can be generalized both to the real world and to the virtual world of the Infosphere using modern information technologies. As a consequence, the separation between public and private spheres tends to disappear. We believe that generalized sousveillance may transform the overall society, e.g. modern public transportation like the Paris subway might have to change the way it disseminates information due to the impossibility of managing the flow of information coming from its infrastructures.*

To attempt to elucidate a society based on generalized sousveillance, the article introduces the notion of the 'Catopticon', derived from Bentham's Panopticon: while the architecture of the Panopticon was designed to facilitate surveillance by prohibiting communication and by installing surveyors in a watchtower, the architecture of the 'Catopticon' allows everybody to communicate with everybody and removes surveyors from the watchtower. The article goes on to explore the opportunities the Catopticon might offer if extended to the whole planet. It also shows the limitations of the extended Catopticon; some are extrinsic: they consist of various resistances which restrict access to the Internet; others are intrinsic: for instance, we can exchange simultaneously only with a few people, while we may have millions of contacts. As a consequence, the various new 'regimes of distinction' mentioned above play a key role in modern societies.

Key words. *Catopticon – Eye tap – Infosphere – JennyCam – Panopticon – Political forms – Privacy – Sousveillance – Surveillance – Transparency*

Social Science Information, 0539-0184; Vol. 49(3): 1–19; 371027

DOI: 10.1177/0539018410371027 http://ssi.sagepub.com

Résumé. *Cet article se fonde sur la notion de 'sousveillance', notion introduite par Steve Mann pour décrire l'état actuel des sociétés technologiques avancées, où n'importe qui prend des photos ou des vidéos de n'importe qui et de n'importe quoi, puis les diffuse, à son gré, au monde entier. L'article explique comment la sousveillance peut être généralisée au monde physique et au monde virtuel de l'infosphère par l'utilisation des technologies contemporaines de l'information. Nous y montrons comment l'usage des technologies de l'information tend à supprimer la séparation entre les sphères publique et privée. Nous expliquons ensuite comment la sousveillance généralisée transforme l'intégralité de la société; par exemple, comment, dans les transports publics comme le métro parisien, on modifie la façon de diffuser l'information du fait de l'impossibilité de gérer de façon centralisée les flux d'information venant des différentes infrastructures.*

Pour tenter d'appréhender les sociétés reposant sur une sousveillance généralisée, l'article introduit la notion de 'Catopticon' qui est dérivée du Panopticon de Bentham: alors que l'architecture du Panopticon était conçue pour faciliter la surveillance en interdisant toute communication et en installant des surveillants dans une tour de guet, l'architecture du Catopticon permet à tous de communiquer avec tous et élimine les surveillants de la tour de guet. Cet article explore les opportunités que le Catopticon offre lorsqu'il s'étend à l'ensemble de la planète. Il expose aussi les limitations du Catopticon étendu. Certaines sont extrinsèques. Elles répondent aux différentes résistances qui restreignent l'accès à l'Internet. D'autres sont intrinsèques. Par exemple, nous ne pouvons échanger simultanément qu'avec très peu de personnes, tandis que nous avons des millions de contacts potentiels. Enfin, nous verrons qu'il existe différents 'régimes de distinction' qui jouent un rôle clef dans les sociétés modernes.

Mots-clés. *Catopticon – Formes politiques – Infosphère – Intimité de la vie privée – JennyCam – Œil-robinet – Panopticon surveillance – Sousveillance – Transparence*

The spectre of *Nineteen eighty-four* (Orwell, 1949) still haunts the contemporary world. With webcams, RFID tags and many other recent information technologies, it now becomes possible to record continuously anybody's daily activities (Bailey & Kerr, 2007). As soon as it is switched on, the mobile phone makes it easy to identify and localize its owner. Location-Based Services (Joore, 2008), which have been perceived as an incredible contribution to individual empowerment, allow for continuous tracking of any movement. With remote-sensing techniques, it is now possible to track people as they change places, even when they decide to resign from public life to cultivate their garden. In many developed countries, personal data concerning health, employment, income, travel and digital communications are officially traced and stored in powerful databases (Lahlou, 2008b). It is then possible to fuse (Laudy, Ganascia & Sedogbo, 2007) all those data using modern data-mining techniques. Many people fear the surveillance society that could result from the generalized use of such techniques.

The notion of a surveillance society may refer to an individual, e.g. a Big Brother, a tribe, a social class, a clan, a militia or any group using the information gathered through surveillance in order to maintain power over others. It indubitably makes sense in a legal state, or at least in a state in which the power-holders need informational arguments to justify their actions. In archaic states, where power was imposed with brute force by a charismatic chief, a king, an emperor or an oligarch, without any other justification, surveillance was not required, except to prevent conspiracies. From this standpoint, surveillance is relatively modern. Prisons, aiming to reform an individual, to teach him the law and to remind him of the necessity to obey it, are also quite recent (Foucault, 1975; Weber, 1969); previously, most of the people convicted were either released or tortured to death. As we shall see, the notion of the Panopticon is emblematic of this new political form that appeared in Europe and North America in the 18th century. Nevertheless, the notion of a surveillance society, which many of our contemporaries still dread, does not seem to characterize the present state of our postmodern societies – at least that is what we intend to show in this article. This does not mean that surveillance has disappeared, but instead that the global organization of the surveillance society has been replaced by a new social organization, more flexible and fluid, where surveillance and what we can call ‘sousveillance’ coexist.

Nowadays, everybody is able to take pictures and record the sounds of everyone else and then disseminate them freely on the Internet; while beforehand the massive development of information technologies, the broad dissemination of information through books, newspapers, radio emissions, TV emissions, movies or photos was the privilege of powerful institutions, such as states or rich companies. In contradiction of the previous state, exclusively governed by surveillance, the new state that we enter is now mainly governed by sousveillance, even if surveillance is still present. This article recapitulates the notion of sousveillance, then shows how the generalization of sousveillance to the whole of society is changing both the way society is organized and its dominant political forms. In addition, many specific social issues of the information society are related to sousveillance and its inherent risks. Most of our contemporaries fear the danger of surveillance, which leads them to focus on ethical issues related to privacy, restriction of freedom and lack of communication. However, as we shall see, many other key social issues are more closely related to the abuses of sousveillance than to surveillance concerns. The coexistence of surveillance and sousveillance leads to a fragile equilibrium that is identified by Steve Mann as a state of ‘equiveillance’. We claim that sousveillance now plays a dominant role in modern societies, which influences the traditional political forms (Manin, 1995; Manent, 2001). By exploring the social and political consequences of a generalized sousveillance, we attempt to analyze the evolutions that follow recent developments in the information sciences and technology from a philosophical point of view and, more particularly, from the perspective of ethics and political philosophy.

The overall organization of the article reflects this argumentation: the first section describes the notion of sousveillance, using some contemporary examples. The following section discusses the generalization of sousveillance to the entire society. It is then shown what the sousveillance society is and how it is distinguishable from the surveillance society. Dedicated to social issues, the third section is divided into two parts, the first addressing well-known social issues of surveillance societies and the second dealing with social issues arising from the sousveillance society. We conclude by discussing such key topics as transparency, the 'right to oblivion' and identity management.

The notion of sousveillance

At the age of 20, Jennifer Ringley placed a webcam in her student room and for 8 years, from 1996 to 2003, disseminated continuously on her website video-recordings of her private life. Her website rapidly became famous: it was visited by more than 3 million people daily, some interested in the sociological implications of such exhibitionism and some in sexual arousal. The success of Jennifer Ringley's website is not an isolated phenomenon. The current development of social networks like Facebook, where members freely make private information available to everybody, attests a similar tendency to exhibit the personal life. Nowadays, many of our contemporaries, especially children and teenagers, are less concerned about privacy and more about authenticity (Manach, 2009). More than anything, they fear anonymity and want to be distinguished from others. Attracting attention is in itself considered important and is worth sacrificing privacy for. More and more we agree to provide access to our intimacy. A continuous record of all individual data, e.g. constitution of personal digital archives, and their free public dissemination through the Web, can also be seen as an example of such tremendous exhibitionism, since every gesture and instant of life is available to everybody. The CARPE research area – acronym for Capture, Archival & Retrieval of Personal Experiences – that is now promoted by the Association for Computing Machinery is an illustration of this tendency to record and make private data available to everybody. If we were in a surveillance society, this type of attitude would have been unconscious and potentially dangerous because authorities would have been able to scan all those records and to take advantage of that information to justify their repression of individuals. However, in our contemporary world, those tendencies have a different interpretation, since they are viewed as freedom.

In parallel to this widespread exhibitionism there exist aspirations to total transparency: there is a movement in favour of data sharing (Peppers & Rogers, 2009) and of data opening. Nowadays, many want public information to be available to everybody. As an answer to this social demand, US President Obama has promoted Government 2.0 (Gov2.0), or Open Government, by making public information about the way public funds are used, about frauds, abuses and public policies. The Website recovery.gov is intended to 'track the money' and to show, on maps, 'where the money is going'. In a similar way, the Website data.gov provides access to all the databases used by public services. For instance, data about the Toxics Release Inventory or clinical drug trials are now accessible to all citizens.

Some argue that this full disclosure of public and private information helps to establish a state of total transparency in society. According to some, for instance Steve Mann, this would not really strengthen the logic of surveillance and lead to a generalized surveillance society, but would instead contribute to institute a new regime, described as a sousveillance (Mann, Nolan & Wellman, 2003), in which powerful people were permanently observed by those they are supposed to dominate. The word sousveillance is a neologism built on the model of 'surveillance', the latter from French *sur*, meaning 'over' and *veiller*, 'to watch', and which literally means 'watching from above'. By analogy, sousveillance has been built to designate the act of watching (*veiller*) from below (*sous*). In the case of sousveillance, the *watchers* are socially below those who are watched, while in the case of surveillance it is the opposite, they are above.

Note that the original notion of sousveillance promoted by Steve Mann signifies that every watcher would voluntarily give free access to all information recorded. Usually, people recording information take part in the event and participants are aware of the recording. According to Steve Mann and to others, this would lead to a more balanced world state of justice, since everybody would act as if he were observed by others (Munro, 2000). Moreover, the sousveillance would help to denounce abuse or to check the conformity of public goods. For instance, Steve Mann shows how, with a camera in his pocket, he can record violation of the electrical code (cf. http://wearcam.org/password-66–450.htm) and make it publicly known. However, in such a case it may happen that people disagree with the information capture and attempt to destroy the camera. On the other hand, if someone has been wrongly accused, it is always possible to show his records in order to be free from doubt. Here, the concept of sousveillance has been generalized to include individuals sharing personal data and anonymous records generated by automatic devices, i.e. security camera systems, video surveillance, CCTV, etc. Accordingly, sousveillance is dependent not only on arbitrary individual wills, but also on the rules by which the automatic recording devices publicly deliver the information they capture.

There are many cases of sousveillance in our contemporary world, since information technologies allow for recording people without their knowledge. For instance, if the police beat up youths in the street or on a subway platform, the use of mobile phones enables every onlooker to record and to publicly diffuse videos of this event. Let us explore a few examples of such sousveillance.

A few examples of sousveillance

On 20 June 2009, during the demonstrations against the results of the Iranian presidential elections, a young woman, Neda Agha-Soltan, was shot. Immediately, her tragic death was video-captured and broadcast over the Internet, which drew immediate international attention; in old totalitarian countries, such information would have been totally ignored. This story characterizes the society of sousveillance, where everything can be seen by everybody, even if those in power prohibit information dissemination. There are hundreds of similar stories. For instance, in Paris's 10th arrondissement on Friday 4 December 2009, two policemen were caught *in flagrante delicto* stealing in a phone shop, and were subsequently indicted for aggravated robbery on the basis of video-surveillance images. The images from a video camera, as revealed by Europe1 (Europe1.fr, 2009), show the two men entering a phone shop in the Rue Louis Blanc and showing a police armband and their professional card. Then, pretending to carry out an identity check, they go behind the counter and steal phone cards before leaving the store… Without those pictures, the two policemen would have never been arrested.

A 25-year-old male, found dead on 30 December 2009, had been arrested for stealing a can of beer in a supermarket near Lyons (France). He was held for two hours by four security guards, who later explained that he suddenly 'lost consciousness' before the police arrived. The security guards were sent to court because of a video-recording that shows a young man pinned against a wall, then against a high table, being punched into unconsciousness. Without such automatic video-records, the security guards would have gone unpunished.

Rachida Dati was the French justice minister from 2007 to 2009, before being elected to the European Parliament in June 2009. This election appears to have been perceived by the former Minister as some kind of exile, and when, after being filmed by the TV channel M6, she forgot to switch off her microphone and called a friend, the ensuing conversation was unwittingly recorded. In the recording Mrs Dati is heard to complain of how tedious it was to live in Strasbourg and to attend the European parliamentary sessions. Her embarrassing remarks were broadcast all over the Web and downloaded by many.

Generalized sousveillance

The generalization of sousveillance to world society as a whole

The foregoing examples clearly show how information technologies transform society: nowadays; everybody is able to capture fragments of information, e.g. pictures, dialogues, videos, etc., using electronic devices like webcams, microphones, mobile phone, RFID, and then diffuse them worldwide, throughout the Web. In the past, only powerful institutions like states or rich companies had the ability to broadcast information on any scale. Since those new techniques enable everybody to be a potential source of information, they appear to promote individual autonomy. Anyone who has something to say to the world can do so freely on the Web. Jeff Jarvis, for instance, in his (2009) book, explains how, while his new Dell computer was out of use, the Dell service after-sales was very inefficient, even though he had contracted a total warranty when he bought it. Moreover, Dell had refused to either offer him a refund or to replace his computer. After Jeff Jarvis mentioned his difficulties with Dell on his blog, which had an incredible impact, sales of Dell computers declined because customers had heard on the Web that the company was not reliable. As a consequence, of the fall in sales, the Dell Company changed its after-sale strategy. From the consumers' point of view, the circulation of such information is very positive, since it helps influence producers and forces them to improve their products and services. But this is not new: in any society, even in the oldest, word of mouth circulated both personal experiences and rumours. What is new today, with modern information technologies, is the scope of this circulation: previously restricted to local areas, e.g. districts, villages or cities, now the scope has been considerably extended. On the one hand, the area in which the information circulates has dramatically increased. From now on, all those who are online, across the entire planet, are quasi-instantaneously reachable by information technologies, which have the potential to connect everybody. On the other hand, people are now directly connected to the Infosphere (Floridi, 2010): they do not shake hands; they use virtual intermediaries, 'inforgs', i.e. informational organisms, in order to get in touch virtually by making their avatar shake hands. Some of those ‘inforgs’ are merely their informational counterparts, which are totally subservient to their will. Others are avatars, which resemble their owner more or less, but which can be present in their absence. Some are even intelligent agents that possess some degree of autonomy. As a consequence, the extension of the sphere of exchanges is now twofold: it has been extended geographically to the entire planet and, from an ontological point of view, from the world of human beings – and more generally, the world of living entities – to the world of ‘inforgs’.

Local surveillance societies, which dominated the 19th and the 20th centuries, have now been replaced by a generalized sousveillance society which reaches incredible proportions, since it not only covers a region, a country or a continent, even the whole world, but also the world of ‘inforgs’.

Surveillance societies were centralized, based on a hierarchical social structure, and localized in a physical building. By contrast, the generalized sousveillance society is equally distributed, strictly egalitarian and delocalized over the entire planet. In order to examine in further depth the structure of this generalized sousveillance society, the following sections discuss an architecture that, in contrast to the architecture of the Panopticon, which was designed for surveillance, is made for sousveillance: this is the ‘Catopticon’.

Panopticon

The Panopticon was designed at the end of the 18th century by Jeremy Bentham as a piece of prison architecture (Bentham, 1838). It was supposed both to decrease the cost of surveillance and to improve its efficiency. Many philosophers, among them Michel Foucault in *Surveiller et punir* (Foucault, 1975), described it as a typical device (*dispositif*) of the modern legal state, i.e. a social arrangement that summarizes the underlying political structure of the society. Briefly, the Panopticon is built on a ring around a central tower, where prison guards can see everything their prisoners do. The cells are transparent, they receive and transmit sunlight. In that way, inspectors may observe the prisoners’ every movement without being seen. Moreover, the prisoners are totally isolated from each other. To summarize, the Panopticon principles are:

- total transparency of the peripheral cells,
- fundamental inequality, which allows the occupants of the central tower, i.e. the observers, to watch all the occupants of the periphery, i.e. the prisoners, without being seen,
- isolation of the prisoners, who can’t communicate with each other.

The extended Catopticon

In a recent article (Ganascia, 2009a), we showed that, by analogy with the Panopticon, which schematizes the surveillance society, generalized sousveillance gives rise to another social arrangement, which we call the 'Catopticon' and which generalizes the notions of 'reflectionism' and 'diffusionism' introduced by Steve Mann (Mann, 1998). The three fundamental principles on which the Catopticon is built can be compared with – and opposed to – the three fundamental principles of the Panopticon:

- total transparency of society,
- fundamental equality, which gives everybody the ability to watch – and consequently to control – everybody,
- total communication, which enables everyone to exchange with everyone else.

In practice, there is no hierarchy, i.e. no central tower, and everyone may communicate in total transparency.

There are many examples that show the existence and modernity of the Catopticon (Ganascia, 2009b). For instance, due to the extensive use of information technologies, the modern subway is a Catopticon, while the classical 20th-century subway was organized on the model of a Panopticon. There are more and more video-surveillance cameras in public spaces in cities, for instance in carparks or on the border between countries, especially in the UK or in the US, but also in France and in other developed countries. However, it is very expensive to examine all the images that are recorded. The number of people that would have to be engaged to efficiently look at those numerous videos is too high. To solve this problem, some authorities decided to allow the whole population to participate in surveillance. For instance, Internet Eyes (http://interneteyes.co.uk/) is an online video-notification system in which any citizen can participate. Everybody can watch pictures transmitted by the cameras from everywhere and notify any 'antisocial behaviours', shoplifting, burglary, vandalism, etc., that they see. The viewers' activities are converted into points according to their usefulness, i.e. depending on their contribution to preventing crimes or to arresting criminals. At the end of the month, the highest-scoring viewers receive reward money. A similar virtual community watch, called BlueServo (http://www.BlueServo.net), has been developed in the United States of America to enlist the public in watching the Mexican border. On this website, everybody, wherever he/she is located in the world, can aid the American customs by watching through the cameras and sensors deployed along the Texas–Mexican border. Note that this extension of sousveillance concerns not only the prevention of crime, but all aspects of social life: at work, at home, as a citizen, etc., everybody participates at each instant of his life in this generalized sousveillance.

In the logic of surveillance that was introduced by Jeremy Bentham, some supervisors had to control the whole society. Here is a totally different logic, where everybody is watching everybody. It is a typical sousveillance organization.

More generally, the contemporary Infosphere is structured primarily as a huge Catopticon (Ganascia, 2009b), which extends both to the entire planet and to the world of informational organisms, i.e. 'inforgs', in Floridi's terminology (Floridi, 2008, 2010). Note that the equality apparent in the architecture of the Catopticon, where the central tower is unoccupied, does not mean that power is equally distributed. New groups are imposing their power in the social space occupied by the Catopticon. However, the legitimization of those new powers is very different from those in the Panopticon. In particular, the authority of knowledge is disappearing.

Coexistence of both an extended Catopticon and multiple extended Panopticons

The formalization of both the Panopticon and the Catopticon helps to prove some general properties of these two social arrangements.

Before going into detail, note that, just as the Catopticon has been extended to the entire planet and to the world of 'inforgs' through the use of contemporary information technologies, the Panopticon can be, too. However, even when it is extended, its properties distinguish it from the generalized Catopticon.

The first property of the generalized Catopticon is its uniqueness. The detailed proof is given in Ganascia (2009a, 2009b). However, the proof is easy to outline: if there were two generalized Catopticons, they would either intersect or not. If there were an intersection, inhabitants of this intersection would have access to both of the generalized Catopticons, which means that everybody in each of the Catopticons would have access to everybody in the other through the inhabitants of the intersection. If there were no intersection, it would mean that the Catopticons were not universal, i.e. that they would not cover the entire planet, which is contradictory.

The second property is that the extended Panopticons may be numerous, even if they are generalized to the entire planet, because each of them is under the arbitrary authority of its centre, and two different Panopticons usually have two different centres.

Lastly, according to the third property, the great Catopticon, which is the generalized Catopticon that has been extended to the entire planet, may coexist with multiple extended Panopticons.

Social issues

Social issues connected with the Panopticon

During the past few years, many of the social issues related to privacy (Lahlou, 2008a) were envisaged under the Panopticon, which acted as a foil, showing what to avoid at all costs. More precisely, the most classical attitudes were motivated mainly by the fear of seeing a Panopticon grow so big that it would cover the entire society. Living in such a huge Panopticon would be a nightmare, since everybody would be under the watch and the domination of the administration, as in a jail, without having the ability to freely communicate with their fellow beings. We must by all means find the way to prevent the realization of such a generalized Panopticon. This has been the horizon of many philosophical approaches. For instance, in the mid-1980s, one of the first works in computer ethics, by Roger Mason (Mason, 1986), summed up the computer ethics topics with the PAPA acronym, which stands for Privacy, Accuracy, Property, Access. All four topics can easily be understood with respect to the characteristic structure of the Panopticon, misuse of which has to be prevented.

Privacy means that each of us has the right to control who consults his personal information and why. It makes sense with respect to the Panopticon structure, where the powerful people, who are inside the tower, have access to all the private information. The aim of privacy is to restrict intrusion into individual private life, distinguishing the private sphere, which is personal, from the public sphere. The notion of privacy marks the limits of the transparency that enables the Panopticon central-power occupants to gather personal information about the peripheral-cell inmates and to misuse it.

The notion of *accuracy* refers to those who are responsible for the authenticity, fidelity and accuracy of information. Similarly, it also refers to those who are accountable for damaging the information or introducing errors. In the Panopticon structure, the central power is the only guaranty, which gives it an incredibly dominant power. It would be appropriate to have independent accreditation institutions that would be responsible for those questions and which would enable each citizen to check all the information he gets.

Property concerns the ownership of information, its price, the rules of its exchange, etc. For instance, what is the price of electronic books or music files? Without going into detail, this makes sense with respect to the structure of the Panopticon, where central-tower occupants are able to define the price and to dictate exchanges.

The last point is *accessibility*, i.e. the nature and the amount of information to which a person or an institution has right of access, and the attendant restrictions of use. Once again, this point takes on meaning only with respect to the dangers of the Panopticon, since the goal is both to restrict the discretionary power of the central-tower occupants and to guarantee right of access to information to the peripheral-cell inmates, who are condemned to a total lack of communication in the original Panopticon structure.

In short, almost all the classical topics of computer ethics have been defined with respect to the structure of the Panopticon viewed as the ultimate danger. As we previously saw, it's true for the PAPA topics, but it's also true for almost all other classical topics.

Social issues connected with the Catopticon

Many modern social issues are not directly related to the Panopticon, but instead to the Catopticon. More precisely, nowadays, the main problems concern not only privacy and the emergence of a totalitarian state in a hierarchical society, but also anonymity and new distinction procedures that help people to emerge in a totally egalitarian society. As previously said, the extended Catopticon exists alongside multiple Panopticons, and therefore the traditional computer-ethics issues, for instance the aforementioned PAPA, are still relevant. However, new social issues are now emerging, and we argue that our role in the present and for the future is to understand them and to try to answer the questions they raise.

To give an idea of those questions, let consider again the PAPA topics, i.e. Privacy, Accuracy, Property, Access, and, with regard to each of them, let us point out the new emerging ethical issues that are related to the extended Catopticon.

In the case of the extended Catopticon, privacy is not the first concern, since the challenge is not to hide, but to emerge from anonymity and to be distinguished from among the vast number of individuals. The success of Jennifer Ringley's website attests this new dimension of society. It is not only the exhibitionism of a young woman that was so successful, but the fact that she had intelligently captured the Zeitgeist. She argued that she wanted to share authentic pieces of her life, which corresponds to the aspiration of many contemporary young people. This made her a famous 21st-century conceptual artist.

The aspiration to show their private life explains why so many people, especially young people, use social networks to share intimacy with their fellow beings. With regard to privacy, i.e. to the right to know who is using your data and why, the question concerns the ability to be recognized and, symmetrically, the right to oblivion. The processes by which individuals distinguish themselves are mainly based on the use of search engines, such as Google, on voting procedures and on reputation establishment, as in eBay.

The economic and political consequences of those 'distinction' procedures are more and more important in the information society. However, many techniques – e.g. 'Spamdexing', which artificially increases the number of references pointing to a Website – tend to bias those distinction processes, which could generate new inequalities, new discriminations, new forms of unfairness and new injustices. Moreover, some want to live a number of different existences on the Web. For instance, they don't want to share the same personal information, and consequently the same identity, with their friends, with their family, with their boss, with their physician, with their insurance company or with their administration. However, it is difficult to avoid contradictions when dealing with multiple identities. This is why researchers are investigating identity management techniques (FIDIS, 2009) which ensure consistency among the different identities.

The notion of accuracy refers to those who authenticate information. In the case of the Panopticon, the ethical challenge was to find independent accreditation institutions – or persons – who are not involved in the government. In the case of the Catopticon, the question is not exactly who – or which institution – is able to validate information, since everybody is independent. It is about trust, i.e. about what makes people trust – or distrust – a person or an institution (Taddeo, 2009).

Property covers the economic aspects of the information society. However, in the case of the extended Catopticon, the economic value is related neither to information nor to goods, but to the attention that has been captured. In other words, we now live mainly in an economy of abundance, where everybody faces many different choices, among which it is difficult to decide. Most of the time, the number of possibilities is so high that individuals do not have the cognitive ability to decide which is best. Choices are often aided by recommending systems, which can easily be biased. Moreover, since the problem is to capture attention, advertisements can be personalized and automatically adapted to individuals according to their history or to their profile. Therefore, while in the Panopticon property referred to the value of information, in the Catopticon, it corresponds to new economic rules, which rely on attention, i.e. on the strategies that help people to retain the attention of their contemporaries and not on strategies that help to sell goods. This raises many ethical questions that we shall not develop here.

The last PAPA topic is access, i.e. the amount and the nature of the information to which anyone can have access. In the case of the Catopticon, everybody potentially has access to all information. Some questions concern accessibility, i.e. the material possibility to access the Infosphere. However, this is no longer a problem, since the number of mobile-phone subscribers reached 4.6 billion worldwide at the end of 2009 (Allard, 2009). One can argue that access to mobile phones is both very difficult and expensive in

Africa and in most third-world countries, which tends to undermine our assertion of globalization. Even if it is still partly true, because big companies artificially increase the cost of communications in poor countries, it appears that the situation is evolving quickly, since numerous telecommunication infrastructures are under development in Africa.

Other questions are related to the restriction of access: when and why can I restrict the access of someone to my personal information. In other words, the information technologies now make it possible to live in a glass-house, where everything is transparent to everybody. However, for social and psychological reasons, this total transparency is not always desirable. One of the most acute ethical issues today concerns the norms on which an ethical justification of opacity can be based (Ganascia, 2007).

H1N1 flu

We support our claims with an example of the way society is changing: the recent episode of H1N1 flu clearly illustrates what it means to live in a Catopticon. During the 19th and 20th centuries, when the Panopticon was the most prevalent figure of social organization, the central administration would have taken authoritarian measures in the light of medical knowledge to ensure social cohesion. Today, many groups and coalitions intervene in the social space, each defending its own interests, while the central state is simply an arbiter. This shows that the hierarchical model of the Panopticon is not an appropriate approach to most social phenomena. More precisely, it shows how those who were traditionally considered to have authority, i.e. politicians, on one hand, and experts on the other, failed to manage the crisis. As a consequence, they were unable to convince the population.

In the following, we shall focus on the history of the recent flu pandemic in France; it appears to have unfolded in more or less similar ways in other European countries.

The main steps of the history of the pandemic can be broken down into four phases: (1) the appearance of the flu pandemic; (2) the political decision; (3) the vaccination plan; (4) the end of the vaccination campaign and the accusations.

1. Appearance of the flu pandemic

(a) Swine flu: the origin is still under debate, but it appeared in April 2009 in Mexico.

(b) Extension in the United States, with a very rapid spread.

(c) The WHO (World Health Organization) launched a very strong signal after three crisis meetings on 24, 27 and 29 April 2009 (early stage 5, late April).
(d) Anxiety in the French populace, who feared a shortage of vaccines.
(e) Criticism addressed to the French health minister, Roselyne Bachelot, who was accused of not having taken strong enough measures.
(f) Installation of individual scanners at airports in some countries – the flu was spreading in the southern hemisphere (austral winter).
(g) Increased production of Tamiflu (an antiviral).
(h) The WHO alert passed to stage 6 (of 7 stages in total), on 11 June 2009.
(i) From 17 July 2009, there was a systematic enumeration by the WHO of infected patients.

2. Political decision

(a) August 2009: pharmaceutical companies announced the development of the vaccine(s).
(b) French health minister decided on a mass vaccination of the population.
(c) French government ordered 90 million doses of vaccine from pharmaceutical companies, which had difficulty fulfilling such a high demand.
(d) Rapid manufacture of millions of doses by pharmaceutical companies.
(e) Emergency procedures presented to the public in France (closing schools, reducing the number of magistrates needed to process a file, etc.).
(f) September 2009: the publication *New England Journal of Medicine* affirmed the effectiveness of vaccines.
(g) The drug-approval procedure of the vaccine was accelerated: the European Medicines Agency approved three vaccines in November 2009.

3. Vaccination plan

(a) Initiation of a vaccination plan: vaccination was not made mandatory, but was accessible from specialized centres throughout the territory.
(b) Exclusion of general practitioners from the plan.
(c) The principle of population vaccination was approved by the majority of experts.

(d) On 19 November 2009, the WHO announced that the vaccine was effective.
(e) Opposition of general practitioners to the vaccination plan.
(f) Nurses declared their hostility to vaccination (fear of risks).
(g) Controversy over the adverse effects of the vaccination.
(h) Failure of the vaccination plan (only 5 million people out of 64 million were vaccinated in France).

4. End of the vaccination campaign and the accusations

(a) Beginning of January 2010 – victory for general practitioners, who obtained the right to vaccinate at their private practices.
(b) Controversies over the vaccination plan and over the cost to the community of the 91 million vaccines ordered.
(c) End of January, challenged by the meeting of the Council of Europe, experts from WHO were accused of having overstated the risks for 'personal reasons'.

This brief history of the flu pandemic shows that the French government, which is traditionally very jealous of its authority in public matters of politics, was unable to follow a strict line. The event that triggered the government's action was undoubtedly the WHO alarm, which, as we know today, was not fully justified. In the traditional logic of sovereignty, i.e. in a state built on the image of the Panopticon, it would have been up to the government to decide for itself when and why it was necessary to act. It clearly appears that such was not the case, since the French attitude was merely a reaction to the WHO alarm and to the anxiety of the population alerted by the media.

For political reasons, such as fear of being accused of inaction by the population, the French government decided to adopt a very active policy in this matter, i.e. to envisage the worst-case scenario and order more than 90 million doses of vaccines, since two doses were believed to be necessary for each citizen. Note that, in an initial phase, many groups accused the government of being inactive or of adopting an inappropriate attitude, and of underestimating the required number of vaccines, which would cause segregation in the vaccination policy.

Then the general practitioners, who were excluded from the vaccination plan, made every effort to cause it to fail. For instance, a French medical website (http://www.atoute.org/), claiming to be an information website and a promoter of Medicine 2.0, circulated a paper (Dupagne, 2010) that was downloaded more than a million times, in which a general practitioner, Dr Dominique Dupagne, compared the risks of the vaccine to the risk of the flu, but omitted to mention the extremely low frequency of vaccine accidents… Moreover, the evaluation of the vaccine's efficiency was in conflict with the official information given out by the EMEA (European Agency for the Evaluation of Medical Products); however, no reference was made to this official evaluation. This paper was countersigned by dozens of other general practitioners and was very influential with the population. Other social groups, for instance hospital nurses, emitted negative advice, while the expert medical advice was only marginally taken into consideration. It is a very new phenomenon that traditional academic authorities have to justify their arguments to non-authorized groups, which are becoming more and more influential. From this standpoint, the social space is no longer a centralized structure orchestrated by a group of authorized persons, i.e. politicians enlightened by academics, which is the image of the Panopticon, but is a completely decentralized environment where multiple social groups oppose each other and where each one goes it alone. In other words, the social space appears to be organized as a typical Catopticon structure.

& & &

To conclude, let us envisage the present evolution: opacity, trust, attention, etc., play a key role in the Catopticon, since they indicate the limits of the transparency that legitimates a totally decentralized organizational structure, i.e. the structure of the Catopticon. For instance, in the case of the recent history of avian H1N1 flu, general practitioners and nurses attempted – and managed – to blur the scientific information given by the academic experts. All those points are new. They raise new questions. Most of them cannot be approached using a classical apparatus. As a consequence, they require new philosophical approaches and new formalizations that could be inspired by philosophers like Georg Simmel (Simmel, 1906). The Catopticon makes those new requirements clear and obvious, thus opening up new areas in the social sciences and clarifying some of the most immediate issues. Certainly, it does not solve those questions, which need new ways of envisaging problems and formulating new conceptualizations. Nevertheless, we argue that investigation of the Catopticon makes it possible to enumerate many of those contemporary social issues.

Jean-Gabriel Ganascia is both a philosopher and a computer scientist. He is presently a professor at the Pierre et Marie Curie University (Paris VI) and a researcher at the computer science laboratory of the Paris VI university (LIP6), where he leads the ACASA team. He originally worked on symbolic machine learning and knowledge engineering. Today, his main scientific interests cover different areas of artificial intelligence: scientific discovery, cognitive modelling, computational philosophy, digital humanities and investigation of creativity. He has published more than 300 scientific papers in conference proceedings, journals and books. In addition, he has published many books and papers on philosophical issues and the social consequences of the development of information technologies, e.g. *L'Ame machine* (Paris: Le Seuil, 2001), *l'Odyssée de l'esprit* (Paris: Flammarion), Voir et pouvoir: qui nous surveille? (Paris: Le Pommier). *Author's address*: LIP6, University Pierre et Marie Curie, 4 place Jussieu, 75005 Paris, France. [*email*: Jean-Gabriel@Ganascia.name]

References

Allard, L. (2009) *Mythologie du portable*. Paris: Le Cavalier Bleu.

Bailey, J. & Kerr, I. (2007) 'The experience-capture experiments of Ringley & Mann', *Ethics and information technology* 9(2): 129–39.

Bentham, J. (1838) 'Panopticon or the inspection house', *The work of Jeremy Bentham*, vol. 4, pp. 37–172. Published under the supervision of his executor, John Bowring. Edinburgh: W. Tait.

Dupagne, D. (2010) 'Faut-il ou non se faire vaccine contre la grippe?'. http://www.atoute.org/n/article134.html

Europe1.fr (2009) 'Two policemen arrested in flagrante delicto of stealing'. http://www.dailymotion.com/video/k2dlgwUImRhr4K1ir4k

FIDIS (2009) 'Future of identity in the information society'. http://www.fidis.net/

Floridi, L. (2008) 'Information ethics, its nature and scope', in J. van den Hoven & J. Weckert (eds) *Information technology and moral philosophy*. Cambridge: Cambridge University Press.

Floridi, L. (2010) *The philosophy of information*. Oxford: Oxford University Press.

Foucault, M. (1975) *Surveiller et punir*. Paris: Gallimard. [*Discipline and punish*, transl. A. Sheridan. New York: Vintage, 1977.]

Ganascia, J.-G. (2007) 'Modeling ethical rules of lying with answer set programming', *Ethics and information technology* 9(1): 39–47.

Ganascia J.-G. (2009a) 'The great Catopticon', in *Proceedings of the 8th international Conference of Computer Ethics and Philosophical Enquiry (CEPE)*, 26–28 June 2009, Corfu, Greece.

Ganascia J.-G. (2009b) *Voir et pouvoir: qui nous surveille?* Paris: Le Pommier.

Jarvis, J. (2009) *What would Google do?* New York: HarperCollins Business.

Joore, P. (2008) 'Social aspects of location-monitoring systems: the case of Guide Me and of My-SOS', *Social science information* 47(3): 253–74. http://ssi.sagepub.com/cgi/content/abstract/47/3/253

Lahlou, S. (2008a) 'Identity, social status, privacy and face-keeping in digital society', *Social science information* 47(3): 299–330. http://ssi.sagepub.com/cgi/content/abstract/47/3/299

Lahlou, S. (2008b) 'Cognitive technologies, social science and the three-layered leopardskin of change', *Social science information* 47(3): 227–51. http://ssi.sagepub.com/cgi/content/abstract/47/3/227

Laudy, C., Ganascia, J.-G. & Sedogbo, C. (2007) 'High-level fusion based on conceptual graphs', in Proceedings of the 10th international Conference on Information Fusion, Quebec, Canada.

Manach, J.-M. (2009) 'La vie privée un problème de vieux cons?', in *Le Monde* 08/06/2009. http://www.lemonde.fr/technologies/article/2009/03/17/la-vie-privee-un-probleme-de-vieux-cons_1169203_651865.html

Manent, P. (2001) *Cours familier de philosophie politique*. Paris: Fayard.

Manin, B. (1995) *Principes du gouvernement représentatif*. Paris: Calmann-Lévy.

Mann, S. (1998) '"Reflectionism" and "diffusionism": new tactics for deconstructing the video surveillance superhighway', *Leonardo* 31: 93–102.

Mann, S., Nolan, J. & Wellman, B. (2003) 'Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments', *Surveillance & society* 1(3): 331–55. http://www.surveillance-and-society.org; http://wearcam.org/sousveillance.pdf

Mason, R. O. (1986) 'Four ethical issues of the information age', *Management information systems quarterly* 10(1). http://www.misq.org/archivist/vol/no10/issue1/vol10no1mason.html

Munro, I. (2000) 'Non-disciplinary power and the network society', *Organization* 7: 679–95.

Orwell, G. (1949) *Nineteen eighty-four*. London: Secker & Warburg.

Peppers, D. & Rogers, M. (2009) 'The social benefit of data sharing', *1 to 1 Media* (January). http://www.1to1media.com/View.aspx?DocId=31350

Simmel, G. (1906) 'The sociology of secrecy and of the secret societies', *American journal of sociology* 11: 441–98.

Taddeo, M. (2009) 'Defining trust and e-trust: old theories and new problems', *International journal of technology and human interaction (IJTHI)* 5(2): 23–35.

Weber, M. (1969) *Economy and society,* edited by Guenther Roth & Claus Wittich. New York: Bedminster Press.