Surveillance and identity
Towards a new anthropology of the person

Chiara Fonio
Università Cattolica – Dpt. di Sociologia
Paper presented at the BSA conference
12-14 April 2007, London

Abstract
In the last decades surveillance and security tools, from cctv to ID cards, have grown to unpredictable levels. From close spaces, such as airports and malls, to urban contexts, our identities have become mere physical features constantly monitored by the penetrating eyes of security devices. The complexity, the nuances and the essential social components of identity are often reduced to ascribed characteristics. Identities have turned into "transparent" and naked bodies, legitimately scrutinised and divided into "pieces". This simplistic approach could lead either to social exclusion of ethnic groups usually associated with deviant behaviour, or to a more general lack of concern for the integrity and the dignity of the person as a whole.
The paper aims at analysing this new and inadequate anthropology of the person by focusing on different examples, such as biometrics and data banks, that emphasise the fragmentation of the body and the risks related to this reductive approach. In particular, the paper describes the outcomes of a qualitative research carried out in the cctv operators control rooms in the city of Milan. My 70 hours observation study has found that the operators mostly monitor ethnic groups (i.e. North-Africans and East Europeans) on the basis of an a priori stigma. In addiction, due to the fact that the majority of the operators are male, women's body is more exposed to the not always discreet electronic gaze.

Introduction

If one aims to map the terrain of the contemporary surveillance society, he or she would notice that is challenging either to draw borders or to identify all the people involved in monitoring processes. Surveillance is an endemic feature of modern life and has grown as a part of being modern (Ball, Wood: 2006). Whilst there are differences among countries, organisations and polices, the worldwide citizens might have experienced one of the many surveillance activities, especially those connected to security: from CCTV to security screening at airports, from ID cards to different kind of tracking, such as online tracing. No matter where one lives: surveillance is a large-scale trend and citizens of many countries already are familiar with checking devices. However, it is misleading, if not unnecessary, to simply state that we all live under pervasive supervision if we do not attempt both to define surveillance and to identify the key issues.

Perhaps the most comprehensive and simple –but not simplistic- definition[1] is the one given by the Surveillance studies network: "The surveillance society is a society which is organized and structured using surveillance based techniques. To be under surveillance means having information about one's movements and activities recorded by technologies, on behalf of the organizations and governments that structure our society. This information is then sorted, sifted and categorized, and used as a basis for decisions which affect our life chances" (2006: 3). This systematic use of routinely collected data is a crucial feature of the world everyday life. There are at least four categories of surveillance: categorical suspicion, seduction, care and exposure (Ball, Webster 2003: 7-8). While the first and the third are concerned with threats and risks either to public security or to health, categorical seduction

[1] For a broad definition see: Lyon (2006).

involves marketing, in particular the aim of tracking the patterns of consumption. Exposure deals with the media and their invasive nature. The previous mentioned categories could be legal, this is the case of passengers screening at airports, or illegal such as wiretapping made by private telephone communication providers. In addiction, surveillance is not always institutionally driven: child tracking, for instance, involves a bottom-up approach to surveillance because it has to do with the desire of concerned parents who wish to locate their children through RFID (Radio Frequency Identification) or Gps (Global Positioning System) systems.

The continuous attention paid to personal information affects several key questions of our private and social experience and those two aspects are mutually interrelated. For example, watching over individual or group of people through CCTV cameras in order to prevent deviant behaviors could have an impact both on privacy (by using digital zooms or biometric devices) and on social identities (such as processes of social categorization or social stigma).

However, I am not concerned here with the whole variety of debate about surveillance. The so called surveillance studies have developed different approaches from a wide range of backgrounds: sociologists (Lyon: 2001; 2002; 2003), along with criminologists (Norris: 1999), geographers (Koskela: 2000;) have offered both extensive overviews of this field, and very specific analysis often connected to empirical evidence or focused on surveillance processes (such as technology, social sorting and data flows) and drawbacks (such as privacy and ethic issues). This paper is about a new anthropology which seems to be fostered by surveillance devices. As Stefano Rodotà argues the massive use of intrusive security tools calls for a new anthropology (2006: 90). The transparent society we live in is populated by new *social objects*, our "naked" bodies legitimately or not scrutinised. There has been a significant shift in perspective: from monitored bodies under the gaze of surveillance public cameras to *modified* bodies through implantable radio frequency identification devices (Rfd) (2006: 89). Social actors have become *networked persons* whose "pieces" (DNA, electronic traces etc…) could be stored, analyzed and assembled in several data banks.

The European Group on Ethics in Science and New Technology has addressed the pervasive influence of information and communication technologies in the opinion No 20 focused on ethical aspects of ICT implants in the human bodies[2]. Surveillance and tracking devices, such as Verichip[3] or the human bar code, are considered potential threats to human dignity, inviolability of the body, psychological integrity and privacy. Beyond the legal background, one can reach the conclusion that not all that is technologically achievable it is also ethically allowable and socially acceptable. The "post-human", such as the one hypothesized in the Microsoft patent number 6,754, 472 (June 2004) which considers the human body as a medium for transmission of data to other machines, is not a future condition. Rather, it is part of an emerging new direction in anthropology and sociology.

The intellectual scope of this paper is, therefore, to address ethical and social issues related to this inadequate and simplistic approach. I will focus both on monitored and modified bodies with the aims of identifying common trends of post-human anthropology. The issues of identity and surveillance are essential in order to analyse the phenomenon.

If the above mentioned shift in perspective is true, it is also accurate to state that there is a lack of concern for the integrity of the person even in apparently less invasive surveillance devices like CCTV. The second part of the discussion will draw on a qualitative research carried out in the CCTV control rooms in the city of Milan, Italy.

[2] http://ec.europa.eu/european_group_ethics/docs/avis20_en.pdf.

[3] Verichip, about the size of a grain of rice, is a human-implantable RFID that contains a 16-digit identifier. The Verichip can correlate the user to information stored on a database for identity verification, medical records access and other uses but does not contains Global Positioning Systems (Wikipedia 2007; http://www.verichipcorp.com/).

Biology versus biography

The proliferation of ICTs in all spheres of life has shown benefits in many areas. In the medical field, for example, active devices are commonly used for patients with heart failures and Parkinson's disease as well as for chronic pain management. Even if they differ in applications, they are generally used to repair deficient bodies capabilities. It seems clear that ICTs, particularly the Internet, have also provided advantages and opportunities in sharing knowledge and overcoming distances constraints, although their benefits are today unequally distributed among countries.

The other side of the coin, is that much of the information produced in the "networked society" (Castells, 1996) is about us. As the European Group on Ethics in Science and New Technology has pointed out "contemporary society is confronted with changes that have to do with the anthropological essence of individuals"[4] (2007: 21). We have witnessed either the rise of the information age or the rise of the transparent society with an unpredictable exposure of sensitive information and threats to the integrity of human bodies due to the extensive use of surveillance devices.

Several international reports have already raised ethical concerns. The survey published by Unesco, focused on ethical implications of emerging technologies, is the most recent and undoubtedly authoritative. In the report ICTs are strictly connected to human rights. As a matter of fact, the so called infoethics goals draw on the Universal Declaration of Human Rights (1948) and primarily deal with privacy and the increasing collection of personal data by private and public entities. The document emphasizes the possible positive effects and the potential negative consequences of many emerging technologies. Specifically, the social implications of biometrics and Rfid, exemplified in two case studies, are central to the discussion I propose here.

Biometric is a technology that measure and analyze unique characteristics (physical or behavioral) of an individual. The measurement of physical characteristics, such as fingerprints, DNA, or retinal patterns, is used to verify the identity of the individuals. Although it could not be considered as a new technology, it is indeed an emerging device that has been extensively used after September 11, 2001 (Lyon 2003). Biometrics could be incorporated into ID cards and security systems, like CCTV, in airports and other public areas and, according to the International Civil Aviation Organization (ICAO), is likely to become a common feature in the globalised world. ICAO, for instance, has been developing a "global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs)".[5] The blueprint is currently adopted by ICAO members and there is evidence to suggest that "universal biometric standards for Machine Readable Travel Documents would evolve into a global mechanism for government sanctioned proof of identity" (Rundle, Colney 2007: 39). Simply stated, it could lead to an international control system able to identify almost everyone. Such a globally unique identifier raises significant privacy and liberty concerns: from the storage of biometrics data to data matching, from error factors in the technology authentication processes to potential abuses of power, from social sorting to mobility regulation and racial discriminations.

Radio Frequency Identification is a device with tracking capabilities: is a generic term for technologies that use radio waves to automatically identify people or objects. It is a tag that transmits a unique identification number that has been applied in various areas. This technology is widely used both in medicine (in particular, chips implanted in patients in order to check on medications) and business (for product tracking). RFID implantation is also used in the employment context (Rundle, Colney 2007: 43) and in leisure environments such as the Baja Beach club in Barcelona where subdermal chips have been offered to VIP customers. The implant, known as VeriChip, offers the advantage to leave

[4] http://unesdoc.unesco.org/images/0014/001499/149992e.pdf.
[5] http://www.icao.int/mrtd/biometrics/recommendation.cfm.

cash and cards at home and pay for drinks (and be identified) using a scanner. RFID it is also being used in transportations and to locate individuals through wearable ICTs devices. In Japan, for instance, child tracking via RFID is nothing new. In the last years there has been a massive public investment in the name of kids security: the tags contained in watches, can be set to send a signal to a Wi-Fi access point used for wireless Internet access; in addiction, they could also be set "to notify parents or guardians automatically via e-mail on a cellular phone or PC if a child passes a specific Wi-Fi access point on the way to or from school"[6]. Biometrics and Rfid technologies have in common the same privacy concerns: from the storage of sensitive data to abuse of power in the workplaces. If they become required by laws, they will likely increase the gap between elite and common people. The issue of their safety is not without controversy: in July 2006, in fact, some hackers proved that they could clone a Verichip implant (Rundle, Colney 2007: 50).

Due to electronic sensors, workplace privacy and employees dignity seem to be at risk. Remote sensing is based on measurement or acquisition of information by a recording device. At International Security Conference West EXPO, in Las Vegas, a new safety tracking system which revolves around a bio-sensor chips, has been recently shown. The system collects information from the reflectance of light on the human body and enables to monitor key vital signs, including heart rate and oxygen saturation levels[7] The SATS (Security Alert Tracking System), is a wearable surveillance device that can be worn as a bracelet or a watch. The purpose of the SATS is to measure unnatural fluctuation in the heart which might be caused by stressful situations, such as "when a person is engaged in unlawful activities". The collected information is sent to a central monitoring system that can be configured with video surveillance cameras in order to determine the source of the stress. What if someone suffers from panic disorders? Panic attacks, for instance, are usually characterized by palpitation, pounding heart and fast heart rates.

Biometrics, Rfid and sensors are only few examples of controversial high technological devices. According to the *Declaration of Principles of the World Summit on the Information Society* (2003), ICTs should seek to create benefits and foster dignity and freedom. The point 58 underlines the respect for human rights "including personal privacy, and the right to freedom of thought, conscience, and religion in conformity with relevant international instruments"[8]. The ethical framework of ICTs is considered fundamental in at least three significant international documents that emphasize the right to the integrity of the person.

The above discussed technological developments have something in common: *they are all relevant to the question of identity*. The latter is a very complex and multifaceted notion, strictly linked to the core issue of the ontology of human beings. When it comes to identity and technology, identification and authentication complicate matter further. Firstly, we should define identity and subsequently attempt to explain the contemporary reductive approach either associated with the importance of identification or biology.

It is challenging to answer the question of who we are because, as Jenkins argues, it is never a settled matter (1996). It is, rather, a dynamic process based on continuous internal and external dialectic: who we are and who are for other people. It is a subtle concept which covers personal and social expectations, status, and opportunities. We identify ourselves, identify other people, distinguish ourselves from others and defined by others. In addiction, personal and social negotiations involved a wide range of situations. I am concerned here with *one* situation: the sense of identity in surveillance societies.

[6] http://www.rfidjournal.com/article/articleview/2050/2/1/
[7] http://www.gizmag.com/go/6961/
[8] http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

Social identity affects processes of reflexivity and interaction. In particular, it is the "way in which individuals and collectivities are distinguished in their social relations with other individuals and collectivities" (Jenkins, 1996: 4). Nowadays this "distinction" is often associated with identification through technology: we live in a permanent state of being identified by proving evidence (in a mall or in a bank) of who we are. Lyon suggests that identification describes uniquely a person in order to demonstrate that he or she is a member of a population (2004)[9]. I would propose that identification deals uniquely with a person to demonstrate whether one is part or not of a specific group: for instance consumer or non consumer (such as club or loyalty cards that recognize the holders), healthy or ill ect... This unique configuration of information is frequently contained in a code. Bogard claims that genetic coding technology is a good example of what identity has become in a monitored (and technologically driven) society (1996). DNA screening, for instance, converts identity in a mere function of the code (1996: 129). Drawing on Nock (1993), he stresses both the impact on privacy and on identity. If social identity is embedded in interaction, what happens when the code replace the various nuances of the self? "I trust you and you trust me because our files (profiles, code) say it's okay to trust oneanother" (*ibidem*), that is *biology replaces biography* and screens substitute for experience. The processes of negotiations dramatically disappear, replaced by the detailed information collected in data banks: if you have the right profile, "you can continue on –with your work, with your relations with others, with your life. If not, you are a target" (1996: 28).

Jenkins distinguishes between a nominal and virtual identity (1996: 24). While the first is the name, the second is the experience, what truly means to bear it. The post-human identity, a broad term that I use in reference to the hypersurveilled identities, is a sort of nominal identity defined by others and made of collections of bits. These fragments, in the form of retinal patters or DNA samples, do not convey information about the person as a whole but rely on a part without considering the entire human being who is monitored. A target is one who does not have a virtual identity made of experiences, cultural background, relationships, rather is one whose biology is more important than biography. The worker who wears the SATS is not someone with health and psychological history, but an employee whose unnatural fluctuations in the heart discloses his or her deviant attitudes. It is quite similar to the genetic determinism approach of the prenatal exams which are supposed to be helpful in identifying potential troublemakers[10]; people would be automatically assigned into "black categories" even before having the chance to live and make their own experiences. A pre-birth label could be extremely hard to confute: everything is scrutinize to single out and "expel" the exceptions.

Surveillance technology might produce meaningful changes in social relationships because of the impoverished notion of identity connected to the extensive use of electronic devices that focus on "pieces" of the body. We have become *networked persons* and we are experiencing the "expropriation" of our body by technology (Rodotà: 2006). It should be noted that it is not a matter of technological determinism, rather the embodiment of social identity is a crucial issue. The notion of the integrity is not irrelevant to the impact of electronic devices. The blind faith in the "mystique" of DNA, or in the disclose world of personal information could lead to reductive approaches that emphasizes biology without paying attention both to the contest and to social aspects of human life. Our embodied identity is far from rooted in a social vacuum. If biology prevails over biography, "the body leaves the life, and the life abandons the body" (Rodotà, 2006: 98). It seems thus imperative to consider the body not only as a medium for the transmission of data, but as an essential component of the complex processes of self-identity and self-identification.

A room with a view

It would be a mistake to assume that the previously mentioned "inadequate anthropology" is mainly connected to emerging technologies, such as ICTs implants. As part of my doctoral thesis, in 2005 I

[9] www.oii.ox.ac.uk/resources/publications/IB3all.pdf

[10] http://news.bbc.co.uk/2/hi/uk_news/politics/5301824.stm

spent 70 hours observing[11] the CCTV operators in 4 different control rooms in the city of Milan, Italy. The outcomes of my research show the above discussed similar risks either of a lack of concern for the monitored person as a whole, and of social categorizations based on an a priori stigma. Before analyzing the results of my ethnographic research, I will briefly describe video surveillance system in Milan.

In the last decade, Milan has witness a considerable increase in the use of CCTV cameras in public space. The first cameras were installed in 1997 to prevent and discourage crime, to promote safe environments, especially green areas and to reduce feelings of insecurity. It should be stressed that, due to a regional law that came into force in 2003, situational crime prevention measures, such as close circuit television, have been financially supported by the Lombardy region. Therefore, there have been significant public investments only in recent years. Since 1997 more than 30 million euros have been spent to install CCTV in "strategic areas" of the city[12]. There are currently nearly 600 cameras in the city which are capillary distributed in parks and "risky areas" such as outskirts and train stations. I am referring here only to the open street CCTV whose cameras are managed by the local authority and staffed by the local police. If one considers the transport center CCTV system both on streets to regulate traffic flows and detect traffic jams and in the underground, the number of cameras is more than 2000. As far as the technological capability is concerned, almost all the dome cameras are digital and use high definition colors as well as powerful zooms. Biometric devices have been unsuccessfully implemented in few cases (such as at the train station). The images are watched by at least two police operators from the control rooms.

The CCTV system is a network: not only are the images monitored at the local control rooms, but they are also visible at the central police station. However, during the day there are no operators who monitor the screen at the central police station. Because the local control rooms close at night, almost 600 hundreds cameras are controlled by one policeman who is located at the central station. Control rooms are situated in the monitored area, although they are not clearly noticeable. The operators are not allowed to leave the control rooms, even of they notice a deviant behavior close to the site.

At present, this case study is the only qualitative research that has been carried out in Italy. Neither quantitative nor qualitative national data focused on video surveillance are available, except for the explorative study carried out in five Italian cities by the Data Protection Authority in 2000[13]. It is no surprising, thus, that the increasing use of CCTV in public places has not caused public debate. Yet few Italian scholars –from criminologists to sociologists- have paid attention to this issue.

Albeit it is not my intention to systematically review the vast literature on CCTV, it should be stressed that most of the research on video surveillance is British. Most likely, as Atkinson claims, because of the rapid rise of CCTV in the United Kingdom over the last decade (Atkinson, 2000). The major empirical studies of video surveillance control room operations have been Norris and Armstrong (1999) and McCahill (2002). After 592 hours of observation Norris and Armstrong have found that the operators target for closer observation individuals who were supposed to belong to a particular social category that is linked with deviant behavior (1999: 103). Their study underlines that suspicion, "based merely on personal characteristic such as dress, race, membership or subculture group" (the so called categorical suspicion) was prevalent (*ibidem*). Operators prejudice determined targeted surveillance and "the gaze of the cameras does not fall equally on all users of the street but on those who are stereotypically predefined as potentially deviant, or who through appearance and demeanour, are

[11] The hours of observations were supplemented by interviews with operators.

[12] http://www.comunemilano.it. The electricity company Aem, which owns an exclusive licence to manage the public lighting, traffic regulation and video surveillance systems on behalf of the Municipality, has installed all the cameras.

[13] http://www.garanteprivacy.it

singled out by operators as unrespectable" (1999: 8). McCahill has found that exclusionary practices were considerably stronger in shopping malls where tracking of non consumers teenagers lead to the ejection from centre.

The research I describe here concerns 4 different sites. The selection of the settings was based on a number of considerations. The most significant is that I choose the most surveilled urban area and that it was not possible to carry out the observations other control rooms. The participant observation aimed to: verify the use of CCTV by operators, by this I mean who was targeted and why; understand the security strategies; understand if and how the operators were trained; identify potential privacy implications. Overall, I aimed to describe the practice of CCTV through a combination of research approach. Due to the small size of the control rooms, it was not always possible to take notes. As a matter of fact, during the observation I sat behind the operators who constantly turned in order to talk to me. I varied days and time to see how the cameras were operated at different time of the week,. Even if being young and female in a work place that is predominantly male did not cause suspicion, the operators were willing to know the aim of the research.

In all the 4 sites, the targeted were young people and women or ethnic minorities associated with criminal deviance. In particular, North-Africans and East European were tracked for no particular reasons but for their appearance. The "border" between being an "object of target" and an "object of an a priori stigma" was slight and the labeling process seemed almost immediate: if one is a member of an ethnic minority is more likely to be watched because he or she is supposed to represent "a risk". Specific socio-construction of deviance were being used by the operators in order to identify drug dealers. One operator, referring to the latter informed me: "who else do we have to monitor? The criminals are all North- Africans". In addiction East- Europeans were labeled as "bad people inclined to steal". Behavioral patterns did not play an important role in determining who had to be monitored. Two social categories were also targeted on the basis of their appearances: young people, in particular those who were poorly dressed and nice-looking women. Women's bodies were more exposed to the electronic gaze[14].

The objects of the target fell into two metaphorical categories: the "transparent bodies" and the "opaque bodies" (Fonio: 2007). The first were legitimately scrutinised bodies through the powerful zooms of the "electronic eyes"; they are passive bodies, opened to an invasive monitoring that could persist even more than 30 minutes. These transparent identities were monitored and tracked; frequently the operators switch among cameras to follow these subjects. North-Africans and East Europeans, along with women and youth belonged to this category. On the contrary the "opaque identities" were non suspicious subjects, specifically Italian men, often business men whose dress code was not perceived as "deviant". In his case study focused on the constructions of deviance among CCTV control room operators in the UK, Smith emphasizes that "certain operatives seemed to link particular items of fashionable clothing to subcultures associated with crime and deviance (e.g. football casuals, ravers, drug addicts and American 'gangster rappers' etc.)" (2004: 386). During my observation, I found that all the operators linked business men look with normality, thus they did not monitor them. These "opaque" identities seemed to go across a "surveillance free area" with a certain amount of privacy in comparison to the above mentioned naked bodies.

Ascribed characteristics, most notably ethnicity and gender, seemed to be the main criteria by which individuals were labelled as targets of surveillance. As a consequence, their bodies became transparent and the operators paid attention to their body parts, such as hands. I experienced one case where a North African man was intensively monitored because he repeatedly touched the grass with his left hand. The operators perceived his gesture as an attempt either to hide drug or to look for

[14] My findings confirm the tendency towards the masculination of space and the objectification of women emphasized by Hille Koskela (2000).

drug in the grass. The panoptic vision is mediated by the electronic eye that, like a deforming mirror, alters the shapes and amplifies the dimensions of body's parts. However, it should be stressed that nobody was ejected from the public area under surveillance: CCTV was mainly used to monitor rather than to exclude. The most serious outcomes are: social sorting, privacy invasion and lack of concern for the integrity and the dignity of the targeted people.

During my observations, I noticed an inclination to a "reality show effect": the lens of the cameras and the screens of the monitors emotionally detached the watchers from the watched. The spatial distance is also a psychological distance and the operators monitored the people as if they were watching a reality show with a low degree of emotional involvement. The operators appeared excluded from the vital processes of the people who compose the city, they watched as spectators, not as citizens.

The privacy of the citizens seemed to be particularly at risk in one site where there are at least 5 cameras installed in front of buildings. I was informed by two operators that they were able to monitor both the entrance of these buildings and "to watch inside several apartments"[15]. The buildings are not exposed to criminal risks, even if they are located in the surounding of the central train station. Furthermore, in all the sites the information notice was either non existent or not provided in the accordance with the mechanisms described in the general provision[16]. In my observation, I frequently noticed a use of the cameras which seemed in breach of the law. In particular, the system is not always proportionate to concrete dangers and video surveillance is not installed after a "careful analysis" and activated "only is other measures are considered insufficient". Instead, CCTV is considered as a universal panacea (with no demonstrable efficacy) in order to prevent and deter crime within the city. On the whole, there is an unnecessary and redundant use of cameras and their potentialities, such as zooms. Video surveillance is thus considered a technological device without social implications: the need for security, along with the need to demonstrate to the citizens that the local municipality "cares" about safety, have lead to rely extensively on surveillance technologies.

Conclusions: towards a new anthropology

ICTs, either emerging technologies or electronic devices such as video surveillance, raise several issues which are relevant to the question of identity. There is no inherent good or evil with surveillance technology[17], but if intelligence and security agencies rely too much on technology without paying attention to the social impacts (even they are unintended effects), one consequence would be an impoverished notion of identity. Bogard argued that we are experiencing the violence of reconstructed and renovated bodies and that "all reflect the current hysteria which surrounds the body today" (1996: 64). Our identities are often assigned to us by a person (such as CCTV operators) or an organization that has been gathering personal information. The main concern is that it is involved a very narrow concept of identity which ignores the social dimensions. The storage of digital representations of unique physical features for identification purposes and the extensive use of zooms in apparently less intrusive devices such as CCTV cameras, have lead to a very simplistic approach.

[15] "To watch inside" means that, if the curtains (or the windows) are open, the operators could zoom in bedrooms and kitchens.

[16] In 2004 the Garante (the President of the Data Commission) adopted a general provision on video surveillance. One of the requirements refers to information given to the data subjects: "Data subjects should be informed that they are going to access or find themselves in an area under video surveillance and that the data are being recorded, as the case may be; this also applies in the case of public events and shows such as concerts or sports events and in connection with advertising activities via web cams". The information notice should be: placed in close to the areas under surveillance, clearly visible and comprehensible.

[17] If these technologies are deployed in a responsible manner, with adequate supervision, public accountability and specific operators training, then some or all of these technologies may become less problematic. After my empirical research the local municipality of Milan asked me to teach the social aspects and privacy implications of CCTV to the operators. This is but one example to show how surveillance devices can be used without sacrificing civil liberties.

Are ascribed characteristics enough to label an individual or a group of people as deviant? Are those characteristics enough to intensively monitor them? Are physical features more important than social aspects? Is the "part" (such as retinal pattern or a hand that belongs to an "unwanted") more significant than the "whole"? If the answer is yes, we are moving forward a new anthropology based on *biology*, rather than on biography. This approach to human beings is decided by technology rather than by men, and social identity is neither the product of negotiations nor the attempt to understand who we are and who the others are, but an act of labelling who enables to divide into predefined standard categories. Not only are we *networked persons*, but also *networked identities* whose body parts are spread in many data banks. This new anthropology redraws both the physical and the social boundaries and impoverishes the notion of the self. The main features are the "revenge" of the body as a medium to transmit data with a lack of concern for the body as a "referent of individual continuity, an index of collective similarity and differentiation, and a canavas upon which identification can play" (Jenkins, 1996: 21).

References

Ball, K. and F. Webster, (eds). 2003, *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Era*, London: Pluto Press

Ball, K and Wood D.M. (eds.) 2006, *A report on the surveillance society* (http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf)

Bogard, W. (1996), The Simulation of Surveillance, Hyper-Control in Telematic Societies, Press Syndicate of the University of Cambridge.

Castells, M. (1996) *The Rise of the Network Society*, New York: Blackwell.

Fonio, C. (2007), *La videosorveglianza. Uno sguardo senza volto*, FrancoAngeli.

Jenkins, R. (1996), *Social identity,* Routledge

Koskela (2000), "The gaze without eyes': video surveillance and the changing nature of urban space in *Progress in Human Geography*, 24: 243–265.

Lyon, D. (2001), *Surveillance Society: Monitoring Everyday Life*, Open University Press.

Lyon, D. (eds) (2002), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, Routledge 2002.

Lyon, D. (2003), *Surveillance after September 11*, Polity Press

Lyon, D. (2004), *Identity cards: social sorting by database* (www.oii.ox.ac.uk/resources/publications/IB3all.pdf)

Lyon, D. (2006), *Surveillance*, The Blackwell Encyclopedia of Sociology (ed. George Ritzer)

McCahill, M. (2002) *The Surveillance Web: The Rise of CCTV in an English City,* Cullompton: Willan.

Nock, S. (1993) The cost of Privacy: Reputation and Surveillance in America, New York: Aldine de Gruyter,

Norris, C., and Armstrong, G., (1999) *The Maximum Surveillance Society: the rise of CCTV* ,Oxford Berg

Rodotà, S. (2006), *La vita e le regole*, Feltrinelli.

Rodotà, S. (2007), *Costruzione del corpo e diritti della persona* in Post-Umano (a cura di Mario Pirreddu and Antonio Tursi: 163-183), Guerini e Associati .

Rundle, M. and Conley C. (2007), *Ethical Implications of Emerging Technologies: a survey* (http://unesdoc.unesco.org/images/0014/001499/149992e.pdf)

Smith, G. J. D. *Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK* (http://www.surveillance-and-society.org/articles2(2)/screens.pdf)