Surveillance & Society
5(2): 102-123
Smart Borders and Mobilities (eds. Amoore, Marmura and Salter)
http://www.surveillance-and-society.org

Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics

Ayse Ceyhan [1]

Abstract

Contemporary security policies are characterized by a dramatic focus on high technology like biometrics as a security enabler. The process of the technologization of security, i.e. the making of technology the centerpiece of security systems and its perception as an absolute security provider, started in the US in the Eighties and has since been expanded to the European Union (EU) and to almost all developed countries. In this process, biometrics is accepted as the ultimate technology to identify people with certainty. This article examines this emphasis on biometrics in France and in the US in the context of the transformations of late modernity and analyses the philosophical and ethical issues that the emphasis on the body as the core element of identification systems raises.

Introduction

Often assumed as a consequence of 9/11, the technologization of security actually finds its roots in the early eighties in the US with the repatriation of Vietnam War devices and their redeployment at the Mexican-American border in 1986 for intercepting smugglers during the "War on drugs."[2] The process continued in the nineties with the problematization of immigration leading to the tightening of border controls against illegal immigration (Andreas 2000; Ceyhan 1997, 2004) and to the constitution of a security continuum linking together drugs, immigration, asylum, crime and terrorism (Bigo 1996). With these early drivers, biometrics was introduced as a technique of the identification of undocumented migrants seeking to (re)enter the US from its Southern border. In addition to biometrics, sensors, motion detectors, long-range and night-vision cameras were installed to capture undocumented migrants during their crossing of the border.

[1] Institut d'Etudes Politiques (IEP), Paris; Director of GEEST (Groupe d'Etudes et d'Expertise sur Sécurité et Technologies). mailto:ayse.ceyhan@sciences-po.org

[2] The term "war on drugs" was first used under the Nixon administration which had decided to deter drugs at the Mexican-American border. In 1986 another "war" was declared by the Reagan administration which under the auspices of an army general was intended to eradicate drug production in Latin America thus stop its smuggling into the US. See P. Andreas, *Border Games .Policing the US-Mexico Divide*, 2001, Ithaca, London: Cornell University Press.

 ISSN: 1477-7487

In the EU, the technologization of security started in the UK with the fight against IRA bombings and expanded to the fight against crime with an emphasis on surveillance. Since the eighties surveillance cameras have been adopted as a device for combating crime and terrorism in public space. In France, the process of technologization started with the securitization of identity documents in the seventies. Suspecting undocumented migrants of being potential identity thieves, France decided to enhance the security features of ID cards by computerizing the basic identifiers required for identifying individuals. In analytical terms, these different steps fit into the process of the widening and deepening of security issues from the traditional military realm to a broad range of focal objects like immigration, borders, identity, welfare, crime and terrorism (Buzan 1991, Waever 1997). These processes accelerated with the end of bipolarity, the progresses of globalization, the expansion of transnationalization and the constitution of a physical and virtual network society (Castells 1997, Dillon 2002).

Identification technologies, surveillance and risk assessment have become the centerpiece of security policies since 9/11. Security technologies which were previously used in pilot programs such as border controls or welfare benefit attributions and on specific, marginal populations (mainly immigrants) have now broadened their scope to embrace the whole population, meaning that all individuals are subject to technological identification and surveillance. Heterogeneous security technologies have been accepted as a universal security enabler by countries participating in the "war against terror" (Lyon 2003; Ceyhan 2005, 2006; Salter 2006, 2007). In this context, with the development of de-territorialized border controls, emphasis was put on the securitization of identification. This was also promoted by the decision of the ICAO (International Civil Aviation Organization) to integrate one of the biometric features - facial recognition, finger print or iris print - in its member states' passports as high a security feature (Doc. 9303). Following this trend, in 2004 the EU adopted the biometric passport for the citizens of the Union and the biometric visa for third country nationals. In addition to these, the US administration's imposition of the biometric passport to foreigners who seek entry into the country contributed to the transformation of biometrics into a global norm of security (Salter 2006).

In this article I will examine the role of technological solutions in contemporary security policies and demonstrate how, in an environment characterized by uncertainty, the unknown and risk generated by globalization and reinforced by September 11, the adoption of electronic identification and surveillance tools is perceived as the ultimate solution for fighting insecurity. What are the rationales of such devotion towards high technology? Is technology a means of securing security in an era of uncertainty (Dillon 1996)? I will draw on examples from France, the US and the EU to examine these questions. I will consider security technologies as devices in the Foucauldian and Deleuzian sense, meaning that they are not only pure artifacts (*technê*) but the assemblage of heterogeneous elements linking the technê together with procedures, regulations, institutions, discourses, perceptions, attitudes etc. (Foucault 1975, Deleuze 1989). This conception enables us to put emphasis on the social, symbolic, organizational and juridical aspects of technology and to investigate how it contributes to the profiling and control of individual and social behaviors.[3]

[3] For a concise but nevertheless sound account of this concept, see Agamben (2007).

Deriving from the Greek *bios* (life) and *metron* (measure), biometrics identifies an individual and authenticates his/her identity by measuring his/her unchangeable body parts like the iris, the retina or the fingerprint, and by storing that information for verification and authentication. With this technology, the inalterable body is transformed into an absolute source of information (Van der Ploeg 1999; Lyon 2001, 2003), which enables authorities to identify people with certainty and trace their movement and itineraries. This information is stored and processed in various databases and, as a consequence, the body is reconstituted as an "interpretative" and "readable text" (Van der Ploeg 1999: 295). However, the focus on the body raises number of critical questions that need to be discussed. What are the consequences of making the body the source and the measure of identification? How does this impact the philosophical and sociological concepts of identity and the relation to the Other?

Security in an Era of Uncertainty

As Lipschutz states, "security demands certainty" (2000: 1). In its formal understanding, certainty means the acceptance of a fact without doubt – a level of confidence attributed to particular knowledge. In the realm of security, what is at stake is not only certainty about the figure(s) of the enemy and about possible threats, but also certainty about the present and future, certainty about the efficiency of the political, economic, strategic and tactical tools that the liberal society produces to be successful. Yet, for realizing this task, liberal societies need opportunities and risks: two elements that are in direct opposition with the certainty and the stability of security. Security analysts try to eliminate uncertainties in order to become more secure. "But risk analysts answer that the cost of eliminating a risk is infinite" (Lipschutz 2000: 1). In this perspective, as he reminds, we can never be totally secure. Security is constantly seeking to establish its markers of certainty and fixity, which are themselves always moving.

There are multiple markers of certainty: the state, the political regime, institutions, borders and boundaries are among the most conventional ones. However some of these, like borders and boundaries, are never fully finalized because they offer the possibility to be crossed and transgressed several times. Others like the state are transforming with globalization losing some of their crucial attributes, like sovereignty (Krasner 1999). Under the pressure of globalization, the traditional Weberian model of a state is becoming more and more difficult to match with material realities (1947). According to this framework, the modern state results from three interrelated processes: 1) the monopolization of the legitimate use of violence and the establishment of a supervisory control of subject populations, 2) the establishment of clear-cut borders and the management of the movements of people inside the territory and at the borders, 3) the establishment of a monopoly over the identification of individuals by the issuance of documents, such as the passport or the ID card (Torpey 2001: 3). However, today, the Weberian model of state territoriality is dramatically challenged by the processes of globalization and transnationalization and the creation of regional entities such as the European Union (EU). In this new framework, characterized by moving borders, access to the territory, and free movement, people are increasingly monitored by a network of

transnational and de-territorialized security agencies, and bureaucracies (Bigo 2000, 2002). In the US and in the EU controls are now processed not only by security agencies and private companies such as the airline carriers, but also by transnational databanks like the PNR (Passenger Name Record) where the profiles of airline travelers are stored and processed in order to assess whether they constitute a security threat (Mitsilegas 2005).

In order to better understand the changes in the markers of certainty, it is worth remembering the dramatic transformation of the concept of security at the end of bipolarity (Buzan 1991). In effect, security is no longer framed by the clear-cut distinction of the inside and the outside but by the inter-penetration of the domestic and the external security realms (Bigo 1996, 2000) and its scope has been deepened and enlarged to new sectors such as the political, the environmental and the societal (Buzan 1991, Waever 1997). In this framework the 'enemy' is not actually the 'Communist' as it was during the Cold War, but has multiple faces. Supposedly it might be the migrant, the citizen with foreign ancestors, the dual-national, the commuter, the poor, the people living in poor suburbs, the foreign student, the anti-globalization protester etc. With 9/11 the terrorist became the overlapping figure. In terms of certainty, this unexpected attack shattered the idea that the US and other Western societies constitute an untouchable power.

Impact of the Transformations of Late Modernity

Drawing on Bauman, Beck and Giddens' work on social insecurity, risk and reflexivity, I consider the transformation of security and the increasing erosion of confidence as the products of the transformations of late modernity. These changes occur under the fluid conditions of globalization and the production of a global risk society generating an increase of perceived uncertainties and insecurities in almost all aspects of life from the intimate setting to global geopolitics.

One of the most important features of late modernity is the transformation of risk, which is the mobilizing dynamic of societies bent on change. As Beck (1992) and Giddens (1999) explained, in the current period, risk assumes a new and peculiar importance. First of all, risk in question is different from its traditional understanding according to which it was supposed to be a way of regulating the future, of normalizing it and bringing it under our domination. But, as Giddens states, "it seems that our very attempts to control the future tend to rebound upon us, forcing us to look for different ways of relating to uncertainty" (3). Risks are no longer experienced as coming from the outside, from the fixities of tradition or nature (external risks), but they are manufactured by the very impact of our developing knowledge about the world. Beck coined the expression "second modernity" to connote the phase marked by the modernity turning upon itself. Manufactured risks are directly influenced by the intensifying globalization and refer to risk situations which we have very little historical experience for confronting. They involve a number of unknowns and their consequences are not yet anticipated. Risks that fall into this category are environmental risks, financial risks, scientific risks, health risks and nuclear risks. The main difference between external risks and manufactured risks is that the latter are not tied to the possibility of calculation, because we do not and cannot know what the real level of risk is. In these circumstances the very act of identifying risks

and defining security becomes subject of struggle between different actors like scientists, politicians, strategists, jurists etc. As the most effective way to cope with the rise of new risks, some propose the adoption of the precautionary principle, while others invent new risk management tools. All these strategies generate an environment of fear and lead to the production of a culture of danger which pervades the entire universe of social and political thought and action. Ericson and Haggerty stress that this impacts considerably the field of policing, treating deviance as a technical problem and thus offering

> procedures and technologies – classification schemes, probability calculations, and communication formats- for dealing with [it] … the threat of crime has become a routine part of modern consciousness, an everyday risk to be assessed and managed in much the same way that we deal with road traffic – another modern danger which has been routinized and 'normalized' over time (Ericson and Haggerty 1997: 39-40).

For Bauman, these transformations occur under the fluid conditions of liquid modernity whose main features are being light, liquid, mobile, slippery, shifty, evasive etc: "Amplified by globalization, the liquid modernity runs out through human and technology networks like communication and information technologies and leak into all aspects of human life" (2000: 14). But these liquid flows lead to the creation of a space that is not colonized either by individuals and citizens and also not controlled by states, generating new fears and anxieties.

Technology has always been a major driver of the great powers' economic and military successes for the past century. In many respects it has been the US' ultimate comparative advantage, enabling their military and technological leadership in an era of "hardware or heavy modernity" (Bauman 2000: 1). During this version of modernity which was the era of territorial rule where the logic of power and the logic of control were both grounded in the strict separation of the inside from the outside, technology was embodied in the logic of growing size and spatial expansion. However, as Bauman reminds "with the technological revolution of the seventies, we moved away from a heavy and solid hardware focused modernity to a light, liquid, software based modernity" (2000: 2-3). This passage has been accompanied by a fundamental shift in the relationship between civilian and defense technology industry. Today, civilian industry is emerging as the driver of many state-of-the-art technologies. High tech devices like biometrics, video-cameras, chips, smart cards, scanners, databases etc., which are not originally military or security devices, are proposed to security agencies as the absolute means to cope with new threats and risks, identify risky people and monitor the flows of the liquid modernity.

The actual move from defense to security technologies results also from the deregulation and privatization of the modernizing tasks and duties. There is a growing voluntary delegation of some of the security tasks to private companies to whom are assigned some of the police surveillance and control duties (Ocqueteau 2004). At the same time, we witness the consolidation of a private security industry not only in the US but also in the EU with an emphasis on the production of biometrics, surveillance cameras, information

and communication technologies etc.[4]

Expanding Technologies

In the context of uncertainty and fluidity, technology is praised to be the very tool to assess dangers and threats, defend against crime and terrorism and monitor the future. After 9/11, the US adopted the idea that to ensure security, emerging technologies must be mobilized to identify threats and intercept terrorists at home and abroad. Calling straightforwardly these technologies "antiterrorism technologies" in the SAFETY Act[5] the US authorized the Department of Homeland Security (DHS) to issue designation and certification for them.[6] Along with this, they created the Homeland Security Advanced Research Projects Agency (HSARPA) as the external research-funding arm of its Science and Technology Directorate. "Its mission is to identify and develop revolutionary technologies, satisfy state, local and federal agencies' operational needs for advanced technology and quickly produce prototypes that lend themselves to commercial applications."[7] Its first priority was to seed the development of the next generation of chemical and biological sensors and systems to meet anticipated threats and unanticipated risks. Among these systems, the government promotes and celebrates identification and surveillance technologies as the absolute tools to assess risks and monitor the future.

Following this trend, the EU laid out in 2003 its security strategy in a document entitled "A Secure Europe in a Better World" in which organized crime, terrorism, state failure regional conflicts and proliferation of weapons of mass destruction were presented as the major threats to security. Positing internal and external security as inseparable, European authorities made the protection of external borders a priority and created for this purpose an external border agency named FRONTEX. At the same time, considering the growing role of technology, they decided to the creation of the European Security Research Advisory Board (ESRAB) to draw the strategic lines for European security research and to advise on the principles and mechanisms for its implementation within the Commission's seventh framework programme for research and technology development (FP7). Covering almost all aspects of security (border security, protection against terrorism and crime, critical infrastructure protection, restoring security in case of crisis etc.) it foresees the improvement of the European security industry and the enhancement

---

[4] The global market share of these technologies is estimated to 120 billion USD with the US at the leading position. However it is worth mentioning the emergence of a European security industry which amounts to 4 billion USD in Germany, and to 3 billion USD in France and the UK each (OECD 2004).

[5] Homeland Security Subtitle G of the Title VIII of the *Homeland Security Act of 2002*: *The Support of Anti-Terrorism by Fostering Effective Technologies Act of 2002* (the SAFETY Act).

[6] The four first antiterrorism technologies that were granted Designation and Certification in July 2004 are: Lockheed Martin Risk Assessment Platform, Michael Stapleton Associates Smart Tech System and Explosion Detection Services, Northrop Grumman Biohazard Detection System, Teledyne Brown Engineering Water Sabre designated to investigate in and aid in the neutralization of explosive.

[7] Statement of Dr Penrose Albright, Assistant Secretary for Science and Technology, Department of Homeland Security, before the Select Committee on Homeland Security, Subcommittee on Cyber Security, Science and research and development, US House of Representatives, October 30, 2003.

of Europe's technological, strategic and operational capabilities.[8]

Among European countries France's attitude to the enhancement of security technologies moved from mitigation to devotion in the year 2000.[9] Actually, security technologies, as an emerging field is quite new in France. Following her tradition of national defense technology producers, especially with companies like Dassault or Thales, France has developed a solid business in military technologies and was seeing security technologies as a by-product of this field. However, with the downsizing of the armies as a consequence of the end of bipolarity and the transformations of the defense economy, French industries started to look at the direction of security and to produce dual-technologies like GPS, sensors and scanners that can be used both for civilian and military aims. Many of these companies like Thales created a security department to produce new technologies for the civilian market. This trend is also generated by the worldwide economic success of certain companies like Sagem, world leader in Automated Fingerprint Identification System (AFIS). In consequence, many of the leading French defense companies have started to produce security technologies for governmental and civilian use. Among these products, the most praised are the biometric identification and authentication technologies. Considering the transformation of identification and surveillance matters into a security issue, the companies' interest in this market is increasing.

Security technologies are characterized by their miniaturization, mobility and connectivity. These features result from the combination of three ranges of technologies: technologies of the living (genetics, biotechnologies, body part prints etc), optical and electronic technologies (laser, glass fiber networks etc) and information and communication technologies (ICT). In their actual deployment they take multiple forms going from "intelligent surveillance systems" to DNA samples, passing by USB keys, chips, sensors, cables, wiretaps, cameras and the Internet etc. Biometrics and smart cards structure the new wave of identification and surveillance methods. At the same time, the boundaries of ICT are rapidly expanding towards many other scientific disciplines in particular biological and life sciences.

The integration of these devices in the security realm is fostered by the interconnection of three logics. First, a logic of security that corresponds to the identification of risks and dangers and to the interception of risky people. Second, a logic of management of flows of people, goods and transportation. And third, a logic of ambient intelligence (*Aml*) which is about the integration of microprocessors in the daily life of individuals to make it more comfortable. In other words, these new technologies move easily between the governmental, securitarian and domestic spheres. They play a vitally important role in the government's attempt to identify people with certainty, assist law enforcement, immigration and border police to identify and intercept terrorists, illegal migrants, illicit drugs etc. and at the same time they expand into commercial and domestic lives to make them more comfortable and intelligent (Ceyhan 2006). As Bauman asserts this happens in

[8] See *Meeting the Challenge: the European Security Research Agenda,* A Report from the European Security Research Advisory Board, 2006.

[9] This section of this article is based on a field research I have been carrying out since 2005 on "Security technologies in France."

the new environment characterized by the move towards a "software-based modernity" (Bauman 2000: 2), where there is an increasing appetite for information in public and private spheres. In this context, information becomes a raw material, it can be processed, altered, multiplied, sold or exchanged through many technological tools, especially like public, private and transnational databases containing personal information about individuals (Marx 1994; Castells 1996; Lyon 2001, 2003).

Emphasis on Identification

According to Hall et al. (1992), late or post modernity is accompanied by a transformation of any fixed or essentialist concept of identity. Drawing on the cultural critic Mercer's observation that "identity only becomes an issue when it's in crisis, when something assumed to be fixed, coherent and stable is displaced by the experience of doubt and uncertainty," he argues that the fragmenting of the cultural, institutional, environmental and symbolic landscapes of the late twentieth century is at the origins of the crisis of identity that we witness today (Hall et al. 1992: 275). However, Bauman states that "to say that modernity has led to disembedding of identity is a pleonasm since at no time did identity became a problem: it was a problem from its birth" (Bauman 1996: 18, 19). This means that from the beginning identity was dramatically linked to take any stable ground and to grow.

Nevertheless in the actual context of uncertainty generated by the end of bipolarity, fluidification of globalization, the dissemination of violence and the attacks of 9/11, identity has once again become a problem. The New York and Washington attacks intensified the dramatic emphasis on identity and identification means and technologies. Since then, knowing with certitude who is who and assigning a recognizable identity to someone, group or entity, have become important tasks for governments and law enforcement agencies. Now more and more governments seek to adopt new technologies of identification like biometrics in order to securitize identities and identification means and to monitor the movements of people inside and across borders.

I define technologies of identification as interrelated systems working together to collect, process, store and disseminate information to support law enforcement agents in their decision-making coordination, control, analysis and visualization. They gather, process and disseminate all identifiers capable of identifying individuals. Their aim is to have a very high standard of documentary proof of identity and identification to provide with certitude who is who and who does or did what. These technologies are finger prints, iris and retina prints, face recognition systems, DNA processing, smart cards that contain extensive personal information, magnetic strips, microchips, visas featuring compact disc technology etc.

But, the most important for our purpose is the computerized databases that keep files containing the print of body parts like the finger, the iris or the retina. Using high-speed networks with advanced intelligence and interconnection, computers can create instant and comprehensive files on millions of people. These databases contribute to the world widening of the "dossier society" that Laudon diagnosed (1986). He has stressed that

through the use of computer records, data storage and the integration of files serving unique programs and policies into more or less permanent national databases, the "dossier society" exposes thousands of officially selected moments in the life of an individual (the citizen, the migrant, the traveler, the commuter, the student, the dual-national citizen etc.) to confront him with the threads of an intricate web of information.

Identification and the Crisis of Identity in France

Even if this explanation, with its focus on computer technologies, may lead to the assumption that the "dossier society" is relatively new, the French historian Noiriel reminds that it was already on its way in France in the ninetieth century as a result of the development of the freedom of movement inside the country (1996, 2001). For him, the constitution of databases and the adoption of identification means are a consequence of the French State formation process. Accordingly, under the Third Republic (1870-1940), the state decided in 1880 to integrate all social classes within the territorial entity and started to shift the barriers it had set against internal immigration (labor classes and peasants were so far forbidden from the free movement inside the territory). This integration was processed in the context of the flourishing of republican ideals of liberty and equality. However this context was not that of peace and security. Indeed, the late nineties were marked by the terrorist actions of French and foreign anarchists exploding bombs and committing political assassinations. It was precisely during these times that an Italian anarchist assassinated the French president Carnot, leading the country into disarray. According to Noiriel, these events created a feeling of security deficit and as a counterpart of the freedom of internal movement it led to the tightening of security measures. Consequently, authorities decided to strengthen the identification means by the constitution and centralization of paper files where different identifiers identifying individuals were stored.

In order to identify criminals, police officers sought to invent new techniques to identify individuals in general and criminals in particular. It is in this context that the French inspector Bertillon, developed in 1879 his "anthropometrical methodology" fixing the uniqueness of a person through the measurement of some of his body parts like the length and the width of the head and some physical features like scars, tattoos etc. This invention is considered by scholars like Piazza as the starting point of modern identification and of biometrics in France (Piazza, 2000). Drawing on Noiriel's work, Piazza examines "the administrative colonization" of French citizens by bureaucratic files and techniques, a process that led to the attribution of a national identity card to French citizens in 1940. Noiriel and Piazza insist that two types of differentiation processed the "carding" (*encartement* in French) of French citizens. First, the differentiation between "good citizens" and "bads" like "the deviants," "the wanderers" and "the poor." Second, the differentiation of national citizens from foreigners who were singled out as being the causes of social, economic and political troubles and as such were put under a special scrutiny via specific police files and documents. In police discourses and practices these two types of differentiation superimposed leading the authorities to search for new technologies for identifying these "risky people" with certainty. Hence, the emphasis on Bertillon's anthropometric techniques.

However, the adoption of the Carte nationale d'identité had not been automatic and generated severe resistances from the population. Yet, even if the fabrication of the ID card has been deeply examined by French scholars, only few explored the resistances that it produced. Examining these, Piazza states that the process of "carding" (encartement) was not widely accepted by the French population and encountered several resistances from the beginning. For instance, in 1921, when the police chief Leuiller decided to include fingerprints in the identity cards, his project was strongly opposed as a practice associating "good citizens" with "offenders" (Piazza 2004: 145-9). Even if after 1968 fingerprints were reintroduced in the ID cards, they were then again suppressed in 1974 on the same basis.

Moreover, the emphasis on identification technologies and on identity has always been transformed into a hot button topic with the problematization of migration, i.e. its transformation into a high political issue in times of deep identity crises. This occurs often systematically each time France's position in international relations is challenged or when she faced severe economic crises like in 1974. Actually, there are many reasons that lead countries to doubt about their identity. For France, one may cite the diminution of her colonial power, the erosion of sovereignty, the loss of her traditional markers of certainty about borders, territory, military service, currency, the actual diminution of her influence within the EU, the autonomization of the civil society, the claims of cultural recognition of third generation Muslim immigrants etc. All these contributed to transform identity into identity problems and identity politics. Emphasizing the reasons of France's doubt about its identity, historian Nora sees the peace installed after the Algerian war as one of its major causes. For him, the overall French identity was dramatically framed by war (not only the Algerian war, but also all the wars France conducted so far). Consequently, the peace signed after the Algerian war marked the end of this cycle and the peace, but instead of being accepted as opening a new era, it was actually "perceived as a defeat." For, it started a new era where the modes of life changed, and the economic activities took a new direction, which impacted the demographic structure making the French population move from agriculture to industry etc. According to Nora, all these constitute one of the main "sources of the confrontation of France with herself" (2007).

This recurrent identity doubt has been generated again with the progresses of globalization, the weakening of traditional borders and the European construction which generated concerns about France's sovereignty and place as a leading country. In the eighties, this doubt led to the transformation of immigration into a security problem which in turn generated a focus on identity documents and the fight against bogus documents. The suspicion on undocumented workers as potential usurpers of identity led to the establishment of unconditional proof of identity. Policy-makers and law enforcement agencies assumed that the lack of a very high standard of documentary proof of identity was leading to a security risk. This led them to adopt new security standards, to tighten immigration laws and border controls and systematize identity checks. With the adoption of new immigration legislation called Pasqua Laws in 1993, French authorities established identity checks not only at the borders but also inside the territory. As for justification, they argued public order concerns as well as the necessity to take compensatory security measures vis-à-vis Schengen agreements which suppressed internal borders and allowed the free movements of EU nationals inside the Union (except

the UK and Ireland).

American Problematization of Immigration

France is not the only country who established a direct securitarian link between immigration and identity under the changes produced by globalization and the end of bipolarity. Almost all nation-states who pushed and at the same time paradoxically resisted globalization found themselves finger-pointing immigrants as the cause of the erosion of national identity. Among them the US who was considered by many as the country where immigration and identity were not seen as a political problem fell into this trap as well in the nineties. This unexpected change started in California with the finger-pointing of undocumented immigrants coming from Mexico and Latin America as the causes of the social and economic problems of this state. Under the pressure of local politicians, Californians adopted in 1994 Proposition 187 transforming undocumented immigrants into illegal beings, denying them public education, public social services and public health care and leading to the stiffening of border controls by the adoption of security programs like Operation Gatekeeper and Hold the Line (Ceyhan 1997; Andreas and Snyder 2000; Nevins 2002). Stressing the need for more secure identity documents, Proposition 187 raised the question of bogus documents presumably utilized by illegal aliens and the criminal stealing of identity documents (especially the Social Security number) and transformed it into a public concern. Hence, two years after the adoption of this state law, its fraudulent document section was largely duplicated into federal law (Illegal Immigration Reform and Immigrant Responsibility Act and Immigration and Nationality Act of 1996). State and federal lists of documents acceptable for establishing identity, employment and welfare eligibility for migrants were established accompanied by an alarming discourse on the proliferation of false documents especially used by illegal migrants. In 1998 the Congress passed a law to criminalize them and the administration decided to adopt high-tech identification means such as biometrics (fingerprint readings, facial and voice recognition systems, hand geometry etc). These technologies became the cornerstone of post-September 11 security measures established with the Enhanced Border Security and Visa Entry Reform Act of 2001.

As Nevins has shown in his analysis of the Operation Gatekeeper,[10] this emphasis on immigration as a problem led to intensify the existential and juridical divides between legal and illegal beings.[11] It also contributed to the introduction of computerized identification systems like IDENT adopted at the Mexican border to facilitate the identification of the expelled people, recidivists and criminals. This logic has been continued and deepened more with the adoption of biometric technologies in the aftermath of 9/11 attacks leading to another divide: good and risky bodies.

[10] Security operation launched under the Clinton administration in October 1994 to seal off a key portion of the Mexican border extending from the Pacific Ocean to San Ysidro check point.

[11] I am referring to the subtitle of his book *[Operation Gatekeeper] The rise of the "Illegal Alien" and the making of the US-Mexico Boundary*, and to Mike Davis' foreword, p. xi.

Biometrics: A Tool for Fixing Certainty

Biometrics is the automated use of physiological, biological, genetic and behavioral features to assess the uniqueness of one person and to determine, verify and authenticate his/her identity. Leaders in the biometrics industry present it as the highly accurate tool to authenticate people and know their identity with certainty. It is celebrated and promoted by the security agencies and politicians as the device that guarantees the decrease of offences based on identity fraud.

However perceiving biometrics' emphasis on identification is not clear at first glance. In effect, in practice, it works like an authentication mechanism, i.e. mechanism of certification attesting the compatibility between the identity document and its holder. By collecting and storing the biological features of an individual (photography, fingerprint, hand, iris, retina or voice sample) that make him/her unique, biometrics fixes the uniqueness of the person in databases. Technically speaking, once a person is registered in the system with one or more physical or behavioral characteristics, this information is processed by a numerical algorithm. The algorithm transforms it into a digital template that is stored in a centralized database which is accessed when "live" images of the finger, hand, face, eye or voice is presented to the system. After a similar algorithmic transformation of this second biometric image, a comparison can be executed. If a matching template is found, the person presenting herself is recognized and counts as known to the system.

As such, biometrics seems to be an authentication process permitting the recognition of a person by the system. But, this in fact conceals its identification objective, i.e. the attribution of a recognizable identity to a person through a process of the distinction between a "risky" and "not risky" person which goes beyond a simple act of authentication. As Muller stresses "…biometric technologies mask the often 'discriminatory' character of this exclusionary move behind its objective, technological, and scientific discourse" (2004: 284). With its apparent emphasis on authentication "in some sense we need not know the friend, but merely authorize access to particular resources, rights and entitlements to the authenticated friends, while blocking the access to the unverifiable" (286).

Identification is actually processed in one or several interconnected databases where information about the individual is transformed into profile(s). It is then compared with information about dangerousness deployed in different files like crime files, border files, terrorist files, DNA databases etc. Through this system, biometrics attributes an identity to a person and accepts or rejects his/her inclusion after having assessed the dangerousness h/she presents. People are categorized as being "safe" or "risky" through automated devices and this, according to Lyon, enables "fresh forms of exclusion that not only cut off certain targeted groups from social participation but do so in subtle ways that are sometimes scarcely visible" (Lyon 2003: 150).

It is worth remembering that biometrics was already used in the ancient China to authenticate property records with fingerprints. Egyptian potters too used fingerprints to authenticate their works. In the nineteenth century, a British officer, Sir William Herschel

utilized the palm print to identify the recipients of welfare benefits in Bengal. As mentioned earlier, it was also in the nineteenth century that biometrics was introduced in policing to identify recidivists criminals by their unchangeable physical characteristics (Alphonse Bertillon's anthropometrics). Since then, it had become the very tool for storing criminal histories. The difference between the ancient and contemporary forms of biometrics rests precisely on the digitization of body part measurements, their storage in databases and use of algorithms to store and compare them with live representations.

9/11 and the Europeanization of Biometrics

At the EU level, biometrics was first adopted in 1997 by the constitution of the database called Eurodac which was designed to control the authenticity of asylum seekers. Created in 1997 but implemented in 2002, Eurodac contains the digitized fingerprint of anyone seeking access to one of the EU countries on the grounds of political persecution.

As Aus notes "under the influence of US 'homeland security,' policy, a treatment that was initially limited to asylum seekers has spilled over to other third country nationals and EU citizens" (2003: 4). Actually, 9/11 brought to surface emphasis on identification and surveillance, generalized them as security issues and draw attention to the relationship between the sovereign and the body (Salter 2006). In effect, after 9/11 the US launched a biometric (Lincoln) visa program to identify people seeking entry to the US. This program was required by the Enhanced Border Security and Visa Entry Reform Act of 2002. Accordingly, except travelers from the 27 visa waiver program (VWP) countries who must present either a machine readable passport (MRP) issued before 2005 or a biometric passport, all persons applying for US visas must have certain biometrics (fingerprints) and digital photographs collected during the visa application interview. This information must be cleared through the DHS Automated Biometric Identification System (IDENT) before an applicant receives a visa. The State Department is continuing to install equipment and software for this program in consulates, but although the technology installation has well progressed, state and the DHS have not developed comprehensive guidance for consular officers. In its report, the Government Accounting Office (GAO) pointed out that consular officers are unclear about whether the fingerprints of applicants should be collected before or during the interview (GAO 2004). As for VWP travelers, the DHS enrolls them in the US Visitor and Immigration Status Indicator Technology (US-VISIT) in all airports and seaports by taking their fingerprint and photograph.

In the EU, a similar procedure has been set by the Schengen Information System II (SIS II), a common European database which will also store the personal data of "unwanted" third country nationals who are not allowed to enter the Shengen Zone, and of "risky" European nationals like those who participate to anti-globalization demonstrations. More recently, Europeans extended this cutting edge technology to visas and decided to complete until 2007 the establishment of a common database named Visa Information System (VIS). Visitors applying for a visa to enter EU countries will increasingly be required to provide biometric fingerprints that will be stored in the VIS database as well as their photography and personal data. France has started to apply a pilot program to implement biometric visas and their database in seven overseas consulates.

Technologically speaking the most commonly used biometric method is the fingerprint. It has been utilized by police forces for almost a century and constitutes 75 per cent of the global biometric market. Then come the facial recognition systems (photography) followed by hand geometry and iris recognition techniques (International Biometric Group 2002). Even if commercially these techniques are presented as infallible, there is however a need to recognize their limitations. Almost all scientific tests and studies conclude that "biometric identification is not perfect, it is never 100 per cent certain, it is vulnerable to errors and it can be 'spoofed.' "[12]

The biometrization of identification documents does not stop at the level of asylum seekers, migrants and tourists but has been extended to the whole population, especially in Europe since identification and surveillance have been erected as crucial security issues. The securitization of identity documents is justified by the increase on identity theft and more intensely as a necessity to fight against terrorism. In this respect, EU member states decided in 2005 to work towards interoperable electronic identification systems under a five-year plan. In the meantime countries like Italy, Belgium, Sweden, Finland and the UK have adopted a biometric identification card for their nationals. Among these the most surprising was undoubtedly the adoption of an ID card for British citizens by the Blair government in 2006. As a country of the common law, the UK had first issued compulsory identity cards during World War I and abandoned them in 1918. They were reintroduced during the Second World War but were abandoned again in 1952. Refusing these cards for almost half a century, the UK yielded under the American pressure towards the introduction of biometric features in identification and travel documents and after the London bombings of 2005 raising substantial data protection and personal privacy concerns. At the same time, security experts claimed that placing such a trust in a single document may make identity theft easier and may make the national identity registration databank an attractive target for computer hackers.

In 2005, France decided to introduce biometric features in the national identity card and to transform it into a smart card having basically two objectives: security and comfort. Called by its initials, the card INES[13] would contain a microchip where the fingerprints and the photograph of the user would be stored and recorded on a central database. The information contained in the card could be acceded by law enforcement agencies and border police. At the same time the card would contain enough security features for certification and economic exchange purposes (a multifunctional card).

However following the resistances generated on the Internet Rights Forum[14] by privacy advocates, human rights organizations, and fundamental rights associations etc, the French government put the implementation of this project on hold. Examining these resistances, Piazza asserts that this time the civil society's opposition "was not only

[12] *Biometrics at the Frontiers:Assessing the Impact on Society*. Report for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), European Communities, 2005, p.10.

[13] Identité Nationale Electronique Sécurisée

[14] A unique experience in Europe, it is a website dedicated to debating Internet utilization and legal and self-regulation issues. Supported by the French government, it is a permanent structure for dialogue, exchange and consultation between users, professionals and institutions.

founded on the trade-off between liberty and security, but also on the limitations of technical capacities, the specificity of chosen identifiers which tend to 'reify' identity and the international character of businesses producing these features" (Piazza 2006: 74).

Identity and the Making of the Body the Site of Identification

Besides technical problems regarding its accuracy, the question raised about biometrics is how this technology participates in the (re)production of identity. Rather than determining any preexisting identity, this method may be better understood as a politics of technological construction of identity (Van den Ploeg 1999; Ceyhan 2004). This technological production of identity is intimately linked to the question of body since with biometrics the body has become the very source of identity and identification (Van der Ploeg 1999; Lyon 2001, 2003; Salter 2006, 2007).

Identity is multi-faceted and assessing it in theoretical terms is quite complex for basically three reasons. First, it is difficult to have an all-encompassing definition of this concept, since its focal objects vary from the Self, the same, the Ego to the individual. Second, its analysis needs a second or even a third concept serving as a vis-à-vis to understand and relativize it. This vis-à-vis may be the category of the Other and/or the concept of alterity. Third, identity is not a mere sociological or philosophical concept. It can be treated through several approaches like phenomenology, hermeneutics, symbolic interactionism, psychology, sociology, structural-genetical approach, anthropology etc.

Since biometrics attempts to equate identity with uniqueness and sameness, we will then tackle this concept through the question of the relationship between identity/Idem and identity/Ipse developed by Ricoeur in his seminal book Oneself as Another (1992). With its aim to assess the uniqueness of a person, biometrics brings identity to the level of Idem, i.e. sameness. Actually the question of sameness is as old as the world exists. In the Antiquity, it intrigued Parmenides and Heraclites who asked precisely how to reconcile identity and change. For Parmenides, it was difficult to conceive change for, if A is no longer A, what is it? Conversely, for Heraclites, everything was in perpetual movement hence his well-known statement "one cannot enter two times in the same river." However, he did not pay attention to the question of individual for the individual, as a sovereign subject did not have a particular place in the Greek thought. H/she was considered as being embedded into the community and what was important was the virtuousness of the human being rather than his/her identity.

Ricoeur calls this emphasis on sameness identity Idem. Thus, sameness denotes permanency, unity (for instance blood group, genes, DNA, biological features). Sameness may indicate a numerical identity, such as oneness or unity (passport number), sameness may denote a qualitative identity such as a resemblance or similarity. Sameness may also denote an uninterrupted continuity or lack of variation, lack of diversity.

Making a distinction between identity as sameness and identity as selfhood, Ricoeur introduces another conception of identity: identity Ipseity. Accordingly the self understands it by being open to otherness and affected by it. It defines the character of an

individual as being an agent of action. Ipseity is the changing component of identity: identity changing with reference to values, norms, and ideals. Identity in interaction with relation to the Other. Identity in movement not fixed and pre-given.

By so doing, Ricoeur examines how selfhood is related to otherness, and how otherness belongs to the meaning of selfhood through a dialogical approach. This understanding is based on an ethical foundation: the individual must be subjected to moral norms, but the respect for norms reaches its full meaning only if it is based on a respect for others. The Other can be understood as my alter ego. It is the mirror in which I reflect myself. Similarly the Other contributes to the structuration of myself and preserves her own alterity. Pluralist democracy privileges this figure: by permitting the individual to think of him/herself as an Other, it protects her from violence.

This understanding is also based on a narrative construction of the Self. A self understood as "the who of a history (story)" the one upon whom the story confers a sort of identity, is a self whose temporalization shapes itself in accordance with a narrative model. Thus Ricoeur introduces the act of "narration" as constitutive of one's identity. In this perspective identity is what produces subjectivity and constructs us as selfhood.

With its mere focus on identity Idem, biometrics introduces a conception of identity which puts aside its dialogical and narrative components developed by Ricoeur and suppresses any relationship to the ethics of the Other (Levinas 1949). It also moves the site of identity from the Self (in relation to the other) to the body itself. This is the body that becomes the very source of identity. However this body is not about the body as the site of subjectivity (Ricoeur) and humanity (Arendt, Bauman) but a reified body without any reference to the Other. Moreover, as Salter contends, within its storage in databases the individual becomes a mobile body and through the interconnection of databases, the passport and the visa system within the institutions of customs and immigration control, the body becomes an internationalized body which has lost control over its subjectivity (Salter 2006: 179).

Moving Bodies

Such a focus on the body makes Salter call for continuing the "serious work that has been done to engage with the scholarship now often known as the 'corporeal turn' in which the body, the social-economic-political conditions of embodied subjectivity, and the relationship between the body and the body politic are taken as important sites of political struggles" (178). As he reminds, several thinkers among whom Foucault took this turn. His emphasis on how body is directly involved in a political field in the disciplinary power (1975) and his examination of biopolitics ground his work. To complete this, it is also essential to take a deep look at how in the Western philosophy of the body and the soul were for a longtime considered as separate and how the body was seen as a site of experiment, inquiry and power.

The infamous separation between the body and soul starts with Plato who sees the body not only as mortal and reproducible but also as generating irrational reactions to impulses

coming from the exterior if it is not well organized. But the philosopher with whom the separation between body (*res extensa*) and soul (*res cogitans*) constitutes a major turn in philosophy is Descartes. Positing the rationality principle at the center of his thinking Descartes focuses on consciousness and reason as constituting the centered self and disregards the body. For him the body is "nothing more than a statute or a machine" (1972). Like we can see it with Locke, rationalist and empiricist traditions adopted this focus on consciousness, which was predominant in philosophy until the previous century. However with anatomists and physiologists like Paré the body was not only considered through an organist approach but was also the site of inquiry about possible pathologies leading to the distinction between the sane/healthy body and the insane/pathologic body.

Under the phenomenological tradition,[15] the body became a focal point in philosophy. In his *Phenomenology of Perception*, Merleau-Ponty attempts to overcome the traditional understanding of the body as an object being opposed to the subject of the self (1945). According to him, the body is both object and subject. It is a lived body where body and consciousness are mediated and it is thus necessary to distinguish between a biological level and a phenomenological level. From the biological perspective, the body is an organic system, and as such it is the place for events of nature, whereas a phenomenological perspective reveals the body as the place where consciousness is manifested through human actions.

The biometrical representation of the body de-links it from consciousness and subjectivity making it a readable text composed of signs and codes. At the same time it operates like an anatomist or physiologist revealing the possible pathologies that it contains. As Van der Ploeg points out, the enrolment of body parts in the biometric system and their comparison against criminal databases, makes the body marked with a sign or stigmata "written by authorities that turn the individual body into a witness against them" (1999: 301). Therefore the body becomes the mark of riskiness and illegality leaving no place to the Other to become the witness of the Self. No place is left to the language, to the narration, to the presence of the Other to assess the Selfhood. As such in the context of uncertainty and fear the body is turning decisively into a source for prediction of actual or future dangers and risks.

Another fundamental concern is about the protection of individuals' right to privacy. What legal framework should be implemented to protect individuals against the intrusion of these technologies in their private life? In the EU, the data protection is framed by the directive of 24 July 1995.[16] This directive is enacted to harmonize laws throughout the EU and to ensure consistent levels of protection for citizens and to allow for free flow of personal information inside the Union. Its key concept is its enforceability and its main tool is the creation of a Data Protection Commissioner or Agency in each member country to enforce the rules.

The EU directive is based on "fair information principle," i.e. openness, access, correction, collection limitation and security. However, even if it constitutes a minimum

[15] Leading figures of phenomenology include: Husserl, Heidegger and Merleau-Ponty.

[16] Directive on the protection of personal data with regard to the processing of personal data and on the free movement of such data.

level of protection, this directive is criticized on three aspects. First, the nature of the data protected. Even if the directive does not make an explicit distinction between private and public data, it does not however provide a sound protection against governmental and security files which process personal information. In effect, governments and security agencies succeed to bypass easily this provision for in practice, security files are often created in secrecy without prior declaration to the Data Protection Agency or Commissioner. It is often after their creation and enforcement (which may last a long time) that they adjust the privacy provision of their files to the EU criteria. This raises crucial issues regarding the protection of the fundamental rights of individuals who are, as we mentioned earlier, almost unaware of the existence of such files. The second problem is about the protection against the transfer of personal data towards third countries like the US. Article 25 of the Directive stipulates that no data transfer towards third countries can be processed provided that these countries possess an "equivalent" data protection regulation. Considering the low-level of protection provided by the US framework which relies on the Privacy Act of 1974, the EU Commission had expressed reluctance about the transfer of the PNR data required by the DHS for authorizing the entry of airline travelers into the country. But the EU could not stand behind its refusal, because of the transformation of the PNR transfer into a condition for entering the American soil by air. Despite the criticisms addressed by the EU Parliament, the EU Commission signed an agreement with the US in 2006 authorizing the data transfer. The third problem concerns the global limits of the Directive's "equivalence" provision. This latter is considered "aleatory" since it cannot provide protection against the free movement of personal data originating from third countries where no similar standard of protection exists.

This turn impacts expressly surveillance systems and practices. Surveillance becomes then a systematic attention to personal data with a view to manage, influence, discipline and monitor people (Marx 1994, 2005; Lyon 2001, 2003). Clarke calls "dataveillance" this systematic monitoring of individual's personal data through the application of information technologies (1988). With these technologies surveillance extends beyond the immediate gaze associated with direct monitoring and becomes more and more "automated, dispensing as far as possible with human operatives" (Lyon 2003: 63). All these make surveillance more focused on risk than on danger. In effect, risk is based on using statistical techniques in order to deduce or infer profiles of people who are not under the immediate gaze of the observer. As Lyon assesses, "Records can be checked and sorted at high speed according to various categories to isolate potential abnormal cases that may indicate risk. [...] This means that they are "algorithmic" or mathematically coded for computers to make "decisions" as to what behavior, signal, word or image fits in which category" (Idem: 63). This shift makes surveillance invisible, leaving no footprints. What is important to stress it that it is processed without the subject's knowledge or consent (Lyon 2001, 2003).

Also, it is worth noting that contemporary surveillance is not the one that operates like the Big Brother but it functions through a network of public, private and transnational databases. More and more it is realized extraterritorially through a network of transnational supervisors like airline carriers, commercial databases, police and intelligence databases. It occurs with neither surveillant nor surveilled fixedness to a single place, and seems to be the convergence of some discrete systems (Amoore 2006). This is why it is described as being organized as an "assemblage" (Haggerty & Ericson,

2000) consisting of multiple and heterogeneous technological items (databases, optical technology, electronics, biology, genetics etc.) that transform human bodies in virtual "data doubles." (Haggerty and Ericson 2000).

Conclusion: Critical Issues

The promotion of technology as a security enabler raises a certain number of crucial critical questions that policy makers who support it do not seem to take into consideration. In effect, new technologies lack a serious evaluation of their reversals, unintended consequences and limits. Moreover, since the systems are still under development, its efficiency and benefits are not accurately evaluated yet. There is a real lack of data and field research about this point. The main question that needs to be raised is the real impact of technology on security – not in terms of perception, but in terms of reality of security provided. In this perspective, the purpose of technology should be clearly addressed. Should technology replace human operators? Should it be just a means for security agencies to deal with violence and insecurity? If so, how will it affect the ways in which they organize their missions? How should it become interoperable with other systems? How will it impact criminal's tactics knowing that they are likely to respond by changing their techniques? For instance, if the only way to get cash is a live finger, criminals will be prone to use violence to get someone's fingerprint. That would considerably change the nature of violence and crime.

These questions need to be addressed not only in terms of the protection of countries against terrorism but also by taking into account the proliferation of identification and surveillance technologies in the daily life of individuals on the domestic and public spheres. Some of these technologies like video-surveillance cameras are intrusive, whereas other technologies like face recognition systems are not. However their aim is the same: distinguishing between 'good citizens' and 'risky people.' The large-scale implementation of these technologies impacts considerably the ways in which people organize their everyday life and the benefit they expect from their implementation. This is prone to generate new (in)security issues necessitating the protection of the individual against the intrusion of this security assemblage in her private life.

References

Agamben, G. (2007) *Qu'est-ce qu'un dispositif*, Paris Payot: Rivages.

Albright, P. (2003) Testimony of Assistant Secretary for Science and Technology, Department of Homeland Security, before the Select Committee on Homeland Security, Subcommittee on Cyber Security, Science and Research and Development, US House of Representatives, October 30, 2003.

Amoore, L. (2006) 'Biometric borders: Governing mobilities in the war on terror,' *Political Geography*, 25: 336-51.

Andreas, P. (2000) *Border Games: Policing the US-Mexico Divide*, Ithaca: Cornell University Press.

Andreas, P and Snider, T. (eds) (2000) *The Wall Around the West: State Borders and Immigration Controls*

in North America and Europe, Boston: Rowman and Littlefield.

Aus, J.P. (2003) 'Supranational Governance in an "Area of Freedom, Security and Justice:" Eurodac and the Politics of Biometric Control,' Sussex European Institute (SEI) Working Paper, no. 72.

Bauman, Z. (1996) "From Pilgrim to Tourist, - or a Short History of Identity," in Stuart Hall and Paul de Gay (eds) *Questions of Cultural Identity*, London, Sage.

Bauman, Z. (1989) *Modernity and the Holocaust*. Cambridge: Polity Press.

Bauman, Z. (2000) *Liquid Modernity*, Cambridge: Polity Press.

Bauman, Z. (2003) *Liquid Love*, Cambridge: Polity Press.

Bauman, Z. (2004) *Identity: Conversations with Benedetto Vecchi*, Cambridge: Polity Press.

Beck, U. (1992) *Risk Society: Towards a New Modernity*, London: Sage.

Beck, U. (1999) *What is Globalization?* Cambridge: Polity Press.

Bigo, D. (1996) *Polices en réseaux : l'expérience européenne*, Paris: Presses de Sciences Po.

Bigo, D. (2000) 'When the Two Become One : Internal and External Securitizations in Europe,' In M. Kelstrup and M. Williams (eds) *International Relations Theory and the Politics of European Integration, Power, Security and Community*, London: Routledge, 171-204.

Bigo, D. (2002) 'Security and Immigration: Toward a Governmentality of Unease,' *Alternatives*, 27: 63-92.

Buzan, B. (1991) *People States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, 2nd edition, Boulder: Lynne Rienner.

Castells, M. (1996) *The Information Age: The Rise of the Network Society*, Vol. 1, Oxford: Blackwell.

Castells, M. (1997) *The Information Age: The Power of Identity*, Vol. 2, Oxford: Blackwell.

Castells, M. (1998) *The Information Age: End of Millennium*, Vol. 3, Oxford : Blackwell.

Ceyhan, A. (1997) 'Etats-Unis frontières sécurisées, identités contrôlées,' *Cultures & Conflits*, 26/27.

Ceyhan, A. (2004) 'Sécurité, frontières et surveillance aux Etats-Unis après le 11 Septembre,' *Cultures & Conflits*, 56.

Ceyhan, A. (2005) 'Policing by Dossier: Identification and Surveillance in an Era of Uncertainty and Fear,' In D. Bigo and E. Guild (eds) *Controlling Frontiers: Free Movement into and Within Europe*, London: Ashgate, 209-32.

Ceyhan, A. (2006) 'Technologie et sécurité: une gouvernance libérale dans un contexte d'incertitudes,' *Cultures & Conflits*, 64: 11-32.

Ceyhan, A. (2006) 'Enjeux d'identification et de surveillance à l'heure de la biométrie,' *Cultures & Conflits*, 64: 13-47.

Clarke, R.A. (1988) 'Information Technology and Dataveillance,' *Communications of the ACM*, 31: 29-45.

Deleuze, G. (1989) 'Qu'est-ce qu'un dispositif,' In *Michel Foucault Philosophe: Rencontre internationale*, Paris: Seuil, 185-95.

Descartes, R. (1972) *Traité de l'homme,* Cambridge: Harvard University Press.

Dillon, M. (1996) *Politics of Security: Towards a Political Philosophy of Continental Thought,* London, Routledge.

Dillon, M. (2002) 'Network Society, network-centric warfare and the state of emergency,' *Theory, Culture and Society*, 19(4): 71-9.

Ericson, R.V. and Haggerty, K.D. (1997) *Policing the Risk Society,* University of Toronto Press.

Foucault, M. (1975) *Surveiller et punir: La naissance de la prison,* Paris: Gallimard.

Garapon, A. and Foessel, M. (2006) 'Biométrie: les nouvelles formes de l'identité,' *Esprit,* Août-Septembre.

Giddens, A. (1991) *Modernity and Self-Identity: Self and Society in the Late Modern Age,* Cambridge, Polity Press.

Giddens, A. (1999) 'Risk,' Reid Lectures, London.

Hall, S., Held, D. and McGrew, T. (1992) *Modernity and its Futures,* Cambridge: Open University Press.

Haggerty K.D. and Ericson R.V. (2000) 'The Surveillant Assemblage,' *British Journal of Sociology,* 51(4) (December): 605-22.

International Biometric Group. (2002) Biometric Market Report, London.

Krasner, S.D. (1999) *Sovereignty: Organized Hypocrisy,* Princeton: Princeton University Press.

Levinas, E. (1987) *Time and the Other,* Trans. R.A. Cohen, Pittsburg: Duquene University Press.

Laudon, K. (1986) *The Dossier Society: Value Choices in the design of National Information System,* New York: Columbia University Press.

Lipschutz, R. (2000) *After Authority: War, Peace and Global Politics in the 21st Century,* Albany: State University of New York Press.

Lyon, D. (2001) *Surveillance Society,* Buckingham: Open University Press.

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

Marx, G.T. (1994) 'The Declining Signification of Traditional Borders and the Appearance of New Borders in an Age of High Technology, Paper for the conference on Georg Simmel Between Modernity and Post modernity, Munich: Ludwig Maximilliams Universidad.

Marx, G.T. (2005) 'Some conceptual Issues in the Study of Borders and Surveillance' in E Zureik, M.B.Salter (eds), *Global Surveillance and Policing. Borders, Security and Identity,* Devon UK and Portland Oregon: Willan Publishing.

Merleau-Ponty, M. (1945) *Phenomenology of Perception,* Paris: Gallimard.

Mitsilegas, V. (2005) 'Contrôle des étrangers, des passagers, des citoyens: surveillance et antiterrorisme,' *Cultures & Conflits*, 58: 155-81.

Mulller, B.J. (2004) '(Dis)qualified Bodies: Securitization, Citizenship and Identity Management,' *Citizenship Studies*, 8(3): 279-94.

Nevins, J. (2002) *Operation Gatekeeper: The Rise of the "Illegal Alien" and the Making of the US-Mexico Boundary*, New York: Routledge.

Noiriel, G. (1992) *Le creuset français: Histoire de l'immigration 19è –2àè siècles*, Paris : Seuil.

Noiriel, G. (1996) *The French Melting Pot: Immigration, Citizenship and National Identity*, Minneapolis: University of Minnesota Press.

Noiriel, G. (2001) *Etat, nation et immigration: Vers une histoire du pouvoir*. Paris: Belin.

Nora, P. (2007) 'Le nationalisme nous a caché la nation,' *Le Monde*, 18-19 March.

Organization for Economic Cooperation and Development (OECD) (2004) 'Security Economy, Economie générale,' *études et prospectives*, 8.

Ocqueteau, F. (2004) *Polices entre État et marché*, Paris : Presses de Sciences Po.

Piazza, P. (2004) *Histoire de la carte d'identité*, Paris: Odile Jacob.

Piazza, P. (2006) 'Les résistances au projet INES,' *Cultures & Conflits*, 64: 65-75.

Ricoeur, P. (1992) *Oneself as Another*, Trans. K. Blamey, Chicago: University of Chicago Press.

Salter, M.B. (2003) *Rights of Passage: The Passport in International Relations*, Boulder, Lynne Rienner.

Salter, M.B. (2006) 'The Global Visa Regime and the Political Technologies of the International Self: Borders, Bodies, Biopolitics,' *Alternatives: Global, Local, Political*, 31(2): 167-89.

Salter, M.B. (2007) 'Governmentalities of an Airport: Heterotopia and Confession,' *International Political Sociology*, 1(1): 49-66.

Schneirder, A. and Ingram, H. (1993) 'Social Construction of Target Populations for Politics and Policy,' *American Political Science Review*, 67(2).

Taylor, C. (1992) *Multiculturalism and "The Politics of Recognition,"* Princeton: Princeton University Press.

Torpey, J. (2001) *The Invention of the Passport: Surveillance, citizenship and the state*, Cambridge: Cambridge University Press.

Van der Ploeg, I. (1999) 'The Illegal Body: "Eurodac" and the Politics of Biometric Identification,' *Ethics and Information Technology*, 1: 295-302.

Waever, O. (1997) *Concepts of Security, Copenhagen*, Copenhagen Institute for Political Science: University of Copenhagen.

Weber, M. (1947) 'The Theory of Social and Economic Organization,' In T. Parsons (ed.) *The Theory of Social and Economic Organization*, Glencose: Free Press.