Humanities and Technology Review
Fall 2015, Volume 34
Pages 28-69
ISSN 1076-7908

LIVING BY ALGORITHM: SMART SURVEILLANCE AND THE SOCIETY OF CONTROL

Sean Erwin
Barry University

Foucault's disciplinary society and his notion of panopticism are often invoked in discussions regarding electronic surveillance. Against this use of Foucault, I argue that contemporary trends in surveillance technology abstract human bodies from their territorial settings, separating them into a series of discrete flows through what Deleuze will term, the *surveillant assemblage.* The surveillant assemblage and its product, the socially sorted body, aim less at molding, punishing and controlling the body and more at triggering events of in- and ex-clusion from life opportunities. The meaning of the body as monitored by latest generation vision technologies formed from machine only surveillance has been transformed. Such a body is no longer disciplinary in the Foucauldian sense. It is a virtual/flesh interface broken into discrete data flows whose comparison and breakage generate bodies as both legible and eligible (or illegible).

Keywords: Deleuze, Foucault, panopticon, surveillance, control society

LIVING BY ALGORITHM

Contemporary discussions on surveillance frequently invoke Foucault’s disciplinary society based on his analyses of Bentham’s panoptic architecture in, *Surveiller et punir*.[1] Whether through street-mounted CCTV cameras or cookies that track search histories, contemporary electronic surveillance would logically seem to intensify the possibilities of the disciplinary society described by Foucault in the 1970s. In fact, many technology commentators take for granted that his conceptual tools provide a sound basis for analyzing contemporary surveillance systems.[2]

However, other analysts hold that coding biases inherent to contemporary surveillance technologies have long called for a re-evaluation of the application of Foucault’s logic of discipline in electronic surveillance contexts. They argue that texts like, *Surveiller et punir*, were important because they focused suspicions on the effect of institutional structures that homogenize social behavior through the feedback set up between the corrective gaze and behavior within the architecture of disciplinary systems.[3] On the other hand, as scholars like Kevin Haggerty (2006, 27) argue digital surveillance technologies do not simply multiply the optics in the panopticon. Driven by software, all electronic surveillance technologies *are programmed.* Scholars like Haggerty point to this fact and claim that changes in surveillance technology have arrived at the point where the panoptic model obstructs progress in understanding of the changes currently taking place; as he states: “…surveillance processes and practices are progressively undermining the relevance of the panoptic model for understanding contemporary surveillance. Foucault continues to reign supreme in surveillance studies and it is perhaps time to cut off the head of the king".[4]

In this paper, I argue that contemporary, post-2000, software-driven surveillance systems are not panoptic in character but distributive, sorting individual bodies into flows through events of in- and exclusion. I also agree with the turn toward Deleuze exhibited by many surveillance commentators critical of Foucault. The analysis Deleuze gives of the shift from disciplinary societies to societies of control in his 1992 essay, "*Post-scriptum sur les sociétés de contrôle*," explains how the interconnectedness of rhizomatic surveillance environments alter the traditional closed panoptic spaces of school, factory, asylum and prison described by Foucault. However, Deleuze and those who champion his paradigm as a replacement to panopticism for theories of surveillance do not fully weigh how surprisingly prone to error these systems are. Surveillant assemblages may appear to extend disciplinary spaces and even to depend on disciplined bodies in order to function but neither the panoptic paradigm attributed to Foucault or the control paradigm attributed to Deleuze address the biopolitical implications of 'smart' surveillance technologies doing the right operations to the wrong things.[5]

II. Foucault and discipline

Panopticism describes a kind of architectural design put forward by Jeremy Bentham in the late 1700s that operates as a machinery of discipline for students, workers, prisoners and the insane. Diffused throughout the social fabric, the panoptic design aims, as Foucault states, “to induce in the detained a state of conscious and permanent visibility that assures the automatic functioning of power”.[6]

Simply by dwelling within panoptic space, inmates internalize the rhythm of movements framed by the prison timetable. In a similar way, schoolchildren in the instructor-monitored classroom rehearse the succession of gestures that pattern competent writing to the point where they come to reproduce them without conscious effort on their part. As a general principle, panopticism distributes power automatically through the arrangement of the space and through explicitly articulated behavioral norms in order to change the behavior of those within the space.[7] The panopticon then functions as a device for conducting conduct. Because the mechanism produces homogenous effects for those within the space, the motive of those responsible for its deployment in a particular context does not matter.[8] Power is exercised with a light touch within such structures, since, in the end, the detained will subject themselves to the directives embedded in the disciplinary structure.[9]

However, current surveillance techniques, though a far cry from an Orwellian Big Brother, set modes of contemporary surveillance apart. Elementary students practicing cursive writing with pen and paper are only monitored by the teacher in the room. Students engaging in the same writing skills using an app downloaded to a tablet may not even need monitoring by a watchful adult, since the app allows proctors to evaluate student engagement without being physically present either during or after the lesson.

Yet the function of these apps is not only to manage student behavior – or at least not their behavior in the classrooms. Their interactions with the app generate data useful to both app designers and marketers. When the traditional student has completed the exercise the paper goes in the trash. What students enter in educational apps have their inputs stored in databases, which form part of their growing, mostly unregulated, digital histories controlled for the most part by private vendors.[10] As they advance through the educational system, these same students may one day respond to polls posted by professors in large university lecture courses on apps downloaded to cell phones. Doing so will add yet another layer of data points for marketers to mine, indicating preferences such as hobbies, career aspirations, diet, voting inclinations, sexual preferences, transportation and housing needs along with assessing their potential tendencies, given a lifetime of inputs, to develop vendor-targeted lifestyle choices.[11]

Surveillance techniques such as big data collection and predictive algorithmic analysis alter the logic of the panopticon[12] by opening it up to the marketplace and the demands of today's data brokers. However today's surveillance data far exceeds the kind of information retrievable from classrooms. It routinely includes video, biometric, geo-demographic and genetic inputs routinely stored by scores of agencies, private and public, in order to track real and virtual behaviors.[13]

Though digital surveillance systems claim to have outsourced Foucault and Bentham's tower guards, studies have shown that these systems exhibit both bias and high tendencies toward error.[14] These characteristics of contemporary surveillance systems make it doubtful whether we are ready to turn over the keys of the tower just yet.

III. Contemporary surveillance as social sorting

Surveillance has conditioned action within urban environments for centuries. In medieval cities walls regulated the flow of townspeople. On high-tech factory lines optical technology autonomously inspects circuit boards.[15]

Contemporary surveillance techniques do not simply direct behavior, but they sort behavior into categories in order to predict future actions. First, digital surveillance relies on databases that use tags to categorize information and make vast data histories culled from electronic records instantly accessible. These data histories act as an electronic 'clone' – or *data double* – of the flesh and blood individual for purposes of electronic surveillance.[16] Distributed to databases across a wide array of networks, these data doubles serve as a nexus for incessant flows of information. Data doubles routinely include everything from pharmacy printouts and notes taken by doctors during routine medical exams to tax reports, banking records, search engine histories, credit card statements and employer files. Searchable databases, and their increasing size and inter-connectedness across different institutions, are key to developing profiles on individuals in industries connected to policing, insurance and marketing.

Despite their global reach databases are not neutral warehouses of information. Database tags categorize the data and, in the process, encode the attitudes and values of stakeholders in law-enforcement, intelligence services, insurance and the financial industries.[17] Information accessed through database searches generates profiles on the basis of these tags and the profiles are key to determining eligibility for reception of benefits, denial of claims, damage awards, permission to travel across borders, employment offers and more. Profilers sift the mountain of data linked to a person's data double for relevance to the litigant, insurance claimant or potential employee under scrutiny.[18]

Coupled with databases, predictive algorithmics drive the assessments that compute future behaviors of bodies. For instance, police rely on predictive softwares to determine the probability of changes in future criminal activity in specific locations to make decisions about whether or not to increase patrols in those neighborhoods. Crunching terabytes of data algorithms project likely storm trajectories for tropical storms forming in the Caribbean. Exploiting minute movements in share price and long-term patterns in markets, computer-powered algorithms endlessly execute purchase and sell orders at the rate of a million per second.[19] From policing to tracking endangered species, contemporary surveillance systems are designed with the goal of predicting individual and group behaviors and forecasting social trends.[20] On the basis of the data doubles associated with individuals,[21] an algorithm generates an assessment of probabilities of that person's likely future behaviors.

Successful behavior prediction depends on effective algorithms driving the software at the basis of the system. Broadly understood, an algorithm is just a set of rules that, when coded, solves a particular problem. The problem for the marketer is to induce those perusing Facebook profiles to click on their ad. In the case of a university recruiting students, the problem is to route the student toward completing a school's application. The algorithm frames a series of prompts in the form of emails, ad windows, and even friendly phone calls from the admissions office to continually re-route the student's attention toward completing the online application form. Thus, if database tags sort things and bodies according to the electronic histories attributed to their data doubles then the algorithm attempts to route them into pre-determined channels framed by the 'if-then' instructions at the heart of the software.

As a mathematical sets of instructions, algorithms would seem to lie outside the realm of bias, much less politics.[22] However, these instructions are generated by individuals within institutions with existing value systems. Advertisers, insurers and the police hold established values regarding the worth of subjects who are young-old, rich-poor, gay-straight, healthy-sick, black-white, male-female. Institutional values determine the variables of the algorithms and serve as the framework for surveillance software that then assesses expected social behaviors by the targeted groups.[23]

As people circulate the sorting process reveals its social biases. Police scan license plates with car-mounted readers as motorists on the freeway pass from home to work. They also conduct the same scans as they patrol high crime neighborhoods where the presence of law enforcement is already more concentrated than in more affluent neighborhoods. Consequently, in these neighborhoods more motorists are stopped and more parked cars are tagged for violations and alerts.[24] On the basis of data histories, scanned passports at immigration kiosks grant easy entry for the majority of visitors while routing alerts to immigration officers who detain or even deny entry to those who have done something as simple as having visited in the recent past a country flagged by the system or accidentally sharing the same name with a serial killer. Some receive credentials, work or insurance benefits while others are denied the same opportunities on the basis of information an employer or social worker inferred from a posting on their Facebook profile.[25] This sort-function is intrinsic to the softwares that drive electronic surveillance networks and its effects go far beyond merely producing data and storing it. As Bogard (2006, 108) states: "Surveillance is not just about collecting information, but decoding and recoding it, sorting it, altering it, circulating it, re-playing it".

Even as designers, vendors and administrators of contemporary surveillance systems claim they monitor environments neutrally, both long term use and competitive testing of these systems has shown the sorting engines at the base of the software can be far from neutral in assessing the actions of bodies.[26] David Introna and Lucas Wood (2004) have explained how the facial recognition systems that form the basis of smart CCTV systems depend on three principal elements: 1) the still or video camera that captures the image; 2) the recognition software that identifies or verifies the probe image on the basis of the type of facial recognition algorithm employed and the database;[27] 3) a human operator to initiate appropriate actions in the case of an alarm or a match.

Bias creeps in through a number of vectors. The facial recognition algorithms reduce facial image data in order to make comparisons with the database. This data reduction causes systems to be biased toward certain types of faces which trigger alerts more frequently when the probe images are compared with those stored in the system's database. Further, the network depends on databases in part generated by geo-demographic inputs that rely on real world urban spaces like neighborhoods and the historical perceptions that law enforcement organizations, marketers and/or insurance companies have of them. Finally, the categories framing the databases depend on tags whose coding is embedded with both designer and client values.

Because surveillance technologies are programmed biases creep in through the terms selected to define database tags and in the way an algorithm's matrix of variables are described. However, since most of this programming forms part of the system's proprietary technology it disappears into a black box that can frustrate detection of these biases in advance. It can prove impossible for even experts to identify what component of a surveillance network – the database, the facial recognition algorithm or both - is the cause of the cascades of false positives being triggered within a given surveillance environment. The presumed function of social sorting is to sift data flows and determine in- and exclusion on the basis of determinations of risk given the individual's data history. Far from constituting a collection of objective, though digitized, facts, a person's data history involves a series of ongoing and complicated translations. Consider for instance an event as simple as taking a person's fingerprint through the use of a biometric scanning device. As Van der Ploeg (1999, 301) states: "The issue of bodily integrity as it relates to biometric technology should not stay focused on the question whether biometric sensors violate the body's integrity by being physically invasive or not. The focus should instead be on the *inscription* of the individual's body with identify/-fiers that is achieved by the combination of fingerprint-taking, storage in a central database, *and* the coupling with biometric sensing equipment and automated searches".

Unlike panoptic surveillance, the actions of the subject within electronic surveillance environments are often irrelevant. For instance, the algorithmic sort-function embedded in Smart CCTV systems are designed to relay to human operators for further scrutiny individuals whose biometrics have already been flagged in the system's databases, as in the case of an individual already known and wanted by law enforcement. However in practice they regularly raise alerts on those with specific sets of physical characteristics, like being dark-skinned and older. Over the history of the system alerts raised on these groups generally prove a succession of false negatives generated by both the system's limitations and factors like poor lighting or crowd conditions that greatly reduce system efficiencies.

As vendor testing of these systems has shown, when deployed in real world environments the majority of the alerts triggered by them have nothing to do with behavior at all.[28] For instance, with facial recognition softwares factors like age, ethnicity and gender of subjects along with the lighting conditions when the images are taken have been shown to greatly affect the comparison of the two sets of images involved – those stored in the database and the probe images taken in the surveillance context for comparison with them.[29] This occurs simply because the facial characteristics of the one show greater variation than the other from the standard facial template that comes bundled with the device. Even detecting individuals already flagged by the system by law enforcement can be notoriously unreliable unless the number of persons actually under surveillance is *greatly* limited *and* environmental conditions are optimum.[30] An older gentleman of Arab American descent has a much greater likelihood of triggering calls for more scrutiny by the system than a 20-something Caucasian woman *already* flagged by the system's software as a person of interest.[31] As Introna and Wood (2004, 188) have shown the error rate for the software that comes standard with CCTV cameras increases considerably in the kinds of conditions one might find in an urban setting or a busy airport.

Contemporary surveillance does not aim to repress. It sorts. For instance it sorts consumers by monitoring consumption patterns, even incentivizing individuals to monitor their own data doubles by providing feedback to augment various social perks such as preferential credit ratings, computer services, or rapid movement through customs. Efforts to evade the gaze of different systems involve an attendant trade off in social rights and benefits and exclusion from life opportunities.[32] Unlike panoptic logics, contemporary surveillance technologies do not aim at conducting conduct or serving as a watchful gaze that evaluates and corrects. Smart surveillance technologies sort by interrupting and re-directing, grouping individuals into flows made more or less predictable on the basis of the digital histories associated with the bodies in the environment under surveillance. Digital surveillance often has very little to do with directly observed, embodied behaviors *at all*.[33] Digital surveillance routes bodies from one environment to the next on the basis of the digital histories tagged to data doubles that represent those bodies within the networks. These events of routing constantly redirect the movements of individuals but they also grant and deny benefits in the process of doing so. The systems are notoriously prone to error often routinely interrupting the movements of individuals for no reason other than the system's own limitations.

IV. Distributed bodies – Deleuze

In his 1992 essay, "*Post-scriptum sur les sociétés de contrôle*",[34] Deleuze argues that for well over a century processes of social ordering have been undergoing a decisive shift, away from architectures of discipline toward a surveillance-based society.[35] Deleuze claims that spaces of disciplinary enclosure have long been in a state of crisis and that a transformation of power has already largely occurred from closed forms of disciplinary organization to open, directed flows monitored by, what he calls, *surveillant assemblages*:

> Individuals have become 'dividuals', and masses

> [have become] - samples, data, markets, or '*banks*'.[36]

In societies of control, both similarities and differences between people are reduced to variations of code. Within the context of contemporary surveillance technology, knowing the body requires its breakdown into a series of discrete data flows that act as a supplement to the flow of bodies through the surveillance context. For this to happen the flesh and blood body must have already been made, as Deleuze terms it, *dividual.*[37] This *dividuality* is at the basis of the shift away from panoptic surveillance to digital surveillance and it happens along two registers: First, biometric interfaces – from facial recognition cameras to iris scanners – are meshed with parts of bodies, transforming them into packets of code. Second, the options open to encoded bodies within networks are laid out *in advance* by the parameters of the algorithms driving these systems.[38]

Flows of flesh and blood bodies through the surveillance context are digitally 'striated',[39] fixed temporally and spatially by the different devices and processes whose co-functioning define the assemblage.[40] For Deleuze, the effectiveness of contemporary surveillance relies on mediating behaviors of real life bodies through networked interfaces that connect the body to webs of information.[41] At the level of the network the result is the digital data double whose data history includes biometric events. Events of biometric striation can be of the discontinuous kind as, for instance, with a fingerprint scan at an airport immigration kiosk. Or, they can be of an 'always-on' variety, like the location tracking many smart phone apps perform automatically.[42]

Given the practical and ontological implications of Deleuze's critique of Foucault in, "*Post-scriptum sur les sociétés de contrôle*", it is evident that the processes embedded in predictive software are not only technical in character but also have clear biopolitical implications for him as well. Critics like Kevin Haggerty and Richard Ericson see advantages to Deleuze's paradigm with its emphasis on rhizomatic linkages, cyborgic human/machine interfaces, and ability to explain features shared by open networks.[43] As Haggerty states:

> …the surveillant assemblage relies on machines to make and record discrete observations. As such, it can be contrasted with the early forms of disciplinary panopticism analyzed by Foucault, which were largely accomplished by practitioners of the emergent social sciences in the eighteenth and nineteenth centuries. On a machine/human continuum, surveillance at that time leaned more toward human observation. Today, surveillance is more in keeping with the technological future hinted at by Orwell, but augmented by technologies he could not have even had nightmares about.[44]

Unlike the traditional panoptic environments described by Bentham and Foucault whose inmates pattern behavioral norms until they have internalized the practices, the operations of sorting, sifting and distributing at the heart of digital surveillance routinely adjust the patterns of lived life according to constantly changing criteria that shift as Deleuzean 'dividuals' pass through different institutional environments.[45]

Deleuze's control paradigm consistently accounts for many of the key features exhibited by today's digital surveillance networks. However, as shown in section ii the sorting engines at the heart of digital surveillance do not simply monitor specific real time behaviors happening within given environments.[46] Where surveillance theorists like Haggerty, Ericson, Lyon and Bogard are right to point to certain advantages the control paradigm forwarded by Deleuze has to the currently dominant panoptic model, they are surprisingly silent about the bias these systems exhibit when they speak about Deleuze. Surveillance networks are designed to function predictively, and they do so by triggering alerts on individuals at least in part on the basis of an individual's 'dividual' physical characteristics like skin color, gender and age that often have no intrinsic connection with the behaviors presumably for which the surveillance is being conducted in the first place. The social sorting they conduct is itself derivative from the base components of digital surveillance – the database and the algorithm – that encode these 'dividuals' and, when combined with biometric inputs, direct bodily flows by triggering events of in- and exclusion often on the basis of these characteristics alone.[47]

At this point a curious fact emerges about the nature of the surveillance conducted by such systems, a fact that is definitely suppressed by vendors and often sidelined by even surveillance commentators. Many of these systems were put into place in the late 90s and early 2000s and have now seen long-term deployments in a variety of urban environments. Over the long term many of these systems have shown an astonishing lack of effectiveness in generating leads on suspects or generating evidence leading to successful prosecutions. Thus, it may come as little surprise that being young, male and black in Britain ensures a higher rate of scrutiny by the UK's 4 to 6 million street-mounted CCTV cameras. However, a comprehensive Home Office report published in 2005 assessing the effectiveness of electronic surveillance in the UK concluded that CCTV coverage was more vendor-driven than results driven.[48] The same report conceded its findings made it possible to conclude the overall ineffectiveness of CCTV as a crime prevention measure in the UK.[49] Similar questions have been raised concerning the effectiveness of CCTV networks deployed in Atlanta[50] and Chicago.[51] Surveillance systems installed at Palm Beach airport and Tampa Bay stadium in Florida were finally dismantled because both systems had failed entirely to register a single genuine security threat while, at the same time, generating an unending stream of false alarms.[52] These last examples involved large scale, expensive surveillance systems that over their life spans were shown conclusively to generate nothing but false positives.[53]

Thus, where Deleuze shows clearly in this short essay that contemporary digital surveillance circulates and sorts bodies through open networks on the basis of how those bodies have been encoded, he does not consider here the significance of the routine failure of digital surveillance to actually positively identify genuine threats or locate persons of interest. If due weight is given to the ubiquity of the false positive in the processing at the basis of these surveillance sorts it becomes clear that determining threat potentials on the basis of real-time inputs actually occurring in the area under surveillance *is not the practical effect of these systems*. The ubiquity of the false positive also further challenges the idea that contemporary electronic surveillance systems function panoptically. If one is effectively subject to interventions no matter how one behaves (or, rather, for no behavior at all and simply on the basis of certain 'dividual' physical characteristics) then such interventions cannot serve as either a positive or negative basis for conducting behavior.

Smart surveillance systems exhibit a startling tendency toward error. However, in the systems described, alerts are forwarded to human operators who can investigate and then intervene to either escalate the alarm or dismiss it as yet another false match. However, latest generation surveillance systems are designed to operate autonomously. In the drive to develop a so-called 'system of systems', the *human monitor itself* has increasingly been replaced by independent, automated visioning systems deployed in the late 90s and early 2000s from the factory floor to the battlefield. Given the often planet-sized quantities of data involved, designers push to automate systems to perform surveillance and sorting functions without a human operator actually present within the surveillance loop. It is important to consider the implications of this latest generation of industrial and military surveillance systems that, on the surface, seem a logical extension of the Deleuzean society of control.

V. The vision machine

Increasing deployment of so-called *closed loop* automated visioning processes has given rise to the dream of a new utopic by designers adapting stand alone vision machines to industrial and military applications since the early 2000s.[54] Considering briefly the objectives of these entirely automated surveillance systems raises pressing questions about the convergence of socially discriminatory sorting processes with startlingly reductionist bio-political agendas embedded in the basic sorting functions of these systems.

Currently, stand alone, AOI vision systems occupy essential roles in networks devoted to industrial, military and space applications.[55] With the AOI system, inspection algorithms utilize millions of data points from an imaging process that uses *structured light* to generate a 3D effect that makes possible comparisons of even complex objects like circuit boards or engine blocks with computer aided design (CAD) models. The algorithms generate assessments on the basis of these comparisons, which allow the visual system to choose the best image generated and to detect, for instance, any deviation of the products from projected results. Systems register even minute imperfections in the morphology and the testing performance of soldered connections on circuit boards and they do this without any person in the loop.[56] Interestingly, an additional, almost Alice in Wonderland, requirement of these machine vision systems is the importance of interfaces for the human operators who work alongside them. These interfaces do not provide people a means to intervene in the production process as they do with alerts raised by smart CCTV systems, since here interfaces are not integral components but only peripherals. They are meant merely to provide constant reassurance to those who work alongside the vision systems that the machines are, in fact, functioning properly.[57]

However, even when coupled with an interactive human interface, automated vision systems generally function through a two-step process that cedes to them relative autonomy. For instance, latest generation navy military helicopters like the *Cyclone* can only function through the automation of visioning made possible by TACCO/SENSO display networks. These systems convert optical images from pick-up devices like camera tubes and vidicons[58] into electronic signals. Signals are then converted into optical symbols on the TACCO/SENSO displays. Pilots read the symbols on the displays but what they read there forms a tiny slice of the total video inputs. The majority of the transferred data has to be automated so as not to overwhelm the pilots overseeing the helicopter's operations.[59]

DARPA's 2003 program, *Combat Zones that See* or *CTS*, claims to engage in a new generation of foreign urban surveillance that sorts, targets and kills in a closed system that requires no human interface.[60] The CTS project intends to render foreign urban battlefields as transparent as open desert by coupling massive computing power with hundreds of thousands of micro- and nano-surveillance devices scattered throughout the urban landscape.

However, CTS goes far beyond the electronic surveillance carried out by Smart CCTV systems, since these earlier generation systems are designed to forward tagged events to human operators who can then determine whether the event warrants further response. Unlike the cameras, the objective of CTS is to automate machine-visioning systems to the point that they instantly communicate interpreted data to other automated systems responsible for targeting and killing. Because of the vast amounts of data involved, this system of systems can only function as designed if no human user intervenes at any point. For Foucault, disciplinary architectures and the panoptic utopia they made possible depended intimately on inmates arriving at the point where they had assimilated the architectural structure and began self-monitoring. If, as Deleuze argues,[61] a shift has already long occurred from panoptic logics to the surveillant assemblages that install the new societies of control, then the objective of designers developing 21st century military surveillance of urban battlefields would clearly no longer aim at conditioning behaviors or producing self-monitoring subjects. Rather, the function of CTS-like systems is of the most biopolitical reductivist kind – to automatically, *predictively* distribute persons toward inclusion in and exclusion from life itself and to whom, why, where or when this will occur may very well be anyone's guess.[62]

REFERENCES

ACLU (2002). Flaws in face-recognition at palm beach airport, *Aclu.org*, 5/14/2002. Retrieved from https://www.aclu.org/news/flaws-face-recognition-palm-beach-airport.

--------(2013). You are being tracked: how license plate readers are being used to track Americans movements. *Aclu.org*, 7/13/2013. Retrieved from https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf

Agamben G. (2004). *Non au tatouage biopolitique*. *Le Monde diplomatique.* January 10, 2004.

Batchelor, B. and Waltz, F. (2001). *Intelligent machine vision: techniques, implementations, applications.* London: Springer-Verlag.

Baumann, N. (2013). Too fast to fail: how high speed trading fuels wall street disasters. *Mother Jones*, Jan/Feb 2013. Retrieved from http://www.motherjones.com/politics/2013/02/high-frequency-trading-danger-risk-wall-street?page=2.

Blau, M. (2012). Atlanta under surveillance. *Creative Loafing*, 12/20/2012. Retrieved from http://clatl.com/atlanta/atlanta-under-surveillance/Content?oid=7121394.

Bogard, W. (1996). *The simulation of surveillance*. New York: Cambridge University Press.

---------(2006). Surveillant assemblages and lines of flight. In Lyon D. (ed.), *Theorizing surveillance: the panopticon and beyond* (97-122). New York: Routledge.

Bosquet, G. (2006). Space, power, globalization: the internet symptom. *Societies* 4, 105-113.

Bowker, J. and Star, L. (1999). *Sorting things out: classification and its consequences*. Cambridge: MIT Press.

Butchart, A. (1996). The industrial panopticon: mining and medical construction of migrant african labour in south africa, 1900-1950. *Social Science and Medicine* 42 (2), 185-97.

Canedy, D. (2001). Tampa scans the faces in its crowds for criminals. *The New York Times,* 7/4/2001. Retrieved from http://www.nytimes.com/2001/07/04/us/tampa-scans-the-faces-in-its-crowds-for-criminals.html.

Carr, Jason (2013). Meet baxter – the $22,000 robot. *Wired Cosmos,* 1/13/2013. Retrieved from http://wiredcosmos.com/2013/01/21/meet-baxter-the-22000-robot/.

Chapman, Steve, (2010). Surveillance cameras a flop. *The Chicago Tribune*, 5/6/2010. Retrieved from: http://articles.chicagotribune.com/2010-05-06/news/ct-oped-0506-chapman-20100506_1_surveillance-cameras-vandalism-effect-on-violent-crime.

Colucci, F. (2010). Cyclone search. *Avionics Today*. 5/1/2010. Retrieved from http://www.aviationtoday.com/av/military/CycloneSearch_67768.html#.Vb0RPu1Viko.

DARPA (2003). Pre-solicitation notice: combat zones that see (cts). Retrieved from https://www.fbo.gov/index?s=opportunity&mode=form&id=9cffd19485baeed4999152d8ac16f3c3&tab=core&_cview=0.

Dennis, B. (2003). Ybor cameras won't seek what they never found. *St Petersburg Times*, 8/20/2003. Retrieved from http://www.sptimes.com/2003/08/20/Hillsborough/Ybor_cameras_won_t_se.shtml.

Deleuze, G. (2003a). *Post-scriptum sur les sociétés de contrôle*. In *Pourparlers. Les éditions de minuit*: Paris, 240-247.

Deleuze, G. (2003b). *Contrôle et devenir* in *Pourparlers*. *Les éditions de minuit*: Paris, 229-239.

Deleuze, G. and Guattari, F. **(**1987). *A thousand plateaus*. Minneapolis: University of Minnesota Press.

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

------------- (2004). *Sécurité territoire population*. Paris: Seuil/Gallimard.

Galloway, A. (2004). *Protocol: how control exists after decentralization*. Cambridge, MA: MIT Press.

Garner, M. (2011). Atlanta police to monitor eyes, ears citywide. *The Atlanta Journal-Constitution,* 2/14/2011. Retrieved from http://www.ajc.com/news/news/local/atlanta-police-to-multiply-eyes-ears-citywide/nQqc8/.

Gilbert, E. (2010). Eye to eye: biometrics, the observer, the observed, and the body politic. In Macdonald, F., Hughes, R. and Dodds, K. (eds.), *Observant states: geopoltiics and visual culture* (225-245). London: IB Tauris.

Gill, M. and Spriggs, A. (2005). *Assessing the impact of cctv.* Home office research study no. 292. London: Home Office Development and Statistics Directorate.

Gordon, D (1987). The electronic panopticon: a case study of the development of the national criminal records system. *Politics and Society* (15:4) 483-511.

----------- (1990). *The justice juggernaut: fighting street crime, controlling citizens*. New Brunswick: Rutgers Press.

Graham, S. (2006a). Cities and the ‘war on terror’. *International Journal of Urban and Regional Research*. 30:2, 255-76.

------------ (2006b). Surveillance, urbanization, and the us revolution in military affairs. In Lyon D. (ed.), *Theorizing surveillance: the panopticon and beyond* (247-269). New York: Routledge.

------------ (2010). Combat zones that see: urban warfare and us military technology. In Macdonald, F., Hughes, R. and Dodds, K. (eds.), *Observant states: geopolitics and visual culture* (199-223). London: IB Tauris.

Haggerty, K. and Ericson, R. (2000). The surveillant assemblage. *The British Journal of Sociology.* 51: 4, 605-622.

Haggerty, K. (2006). Tear down the walls: on demolishing the panopticon. In Lyon, D. (ed.), *Theorizing surveillance: the panopticon and beyond* (23-45). New York: Routledge.

Home Office/ACPO (2007) *National cctv strategy.* London: Home Office.

Haraway, D. (1991). *Simians, cyborgs and women: the reinvention of nature*. New York: Routledge.

Introna, D. and Wood, L. (2004). Picturing algorithmic surveillance: the politics of facial recognition, *Surveillance Studies*. 2:2/3, 177-198.

La Vigne, N; Lowry S.; Markman, J.; Dwyer, A. (2011). Evaluating the use of public surveillance cameras for crime control and prevention – a summary. *Urban Institute,* 9/19/2011. Retrieved from http://www.urban.org/research/publication/evaluating-use-public-surveillance-cameras-crime-control-and-prevention-summary.

Lianos, M. (2003). Social control after foucault. *Surveillance and Society*, 1 (3): 412-430.

Lord, R. and Henney, M. (2015). Surveillance society: students easy target for data miners. *Pittsburgh Post Dispatch*, 8/20/2015. Retrieved from http://www.post-gazette.com/news/surveillance-society/2015/08/20/Surveillance-Society-Students-easy-targets-for-data-miners/stories/201508230018.

Los, M. (2006). Looking into the future: surveillance, globalization and the totalitarian potential. In Lyon, D. (ed.), *Theorizing surveillance: the panopticon and beyond* (69-94). New York: Routledge.

Lyon, D. (1993). An electronic panopticon? a sociological critique of surveillance theory. *The Sociological Review*, 41(3).

--------- (2003). *Surveillance as social sorting: privacy,* *risk and digital discrimination*. London and New York: Routledge.

--------- (2006). *Surveillance studies: an overview*. Cambridge, UK: Polity Press.

Mann, S; Nolan, J; and Wellman, B (2003). Souveillance: inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance and Society*, 1 (3), 331-55.

Mathiesen, T. (1997). The viewer society: michel foucault's 'panopticon' revisited. *Theoretical Criminology*, 1(2), 215034.

Newman, S. (2009). Politics in the age of control. In Poster, M. and Savat. D. (eds.), *Deleuze and new technology* (104-122). Edinburgh: Edinburgh UP.

Norris, C. and G. Armstrong (1999). *The maximum surveillance society, the rise of cctv*. Oxford: Berg.

Poster, M. (1990). *The mode of information: post-structuralism and social context*. Chicago: University of Chicago Press.

Patton, P. (1994). Metamorphologic: bodies and powers in *a thousand plateaus*. *Journal of the British Society for Phenomenology* 25(2): 157–169.

Reese, R. (2011). Police blue light cameras not deterring the most violent crimes. *Medill Reports: Chicago*, 2/10/2011. Retrieved from http://news.medill.northwestern.edu/chicago/news.aspx?id=178125.

Rehagen, T. (2013). Inside the apd's video surveillance room. *Atlanta Magazine*, 5/1/2013. Retrieved from http://www.atlantamagazine.com/news-culture-articles/apd-video-surveillance/.

Shachtman, N. (2003). Big brother gets a brain. *Village Voice*, 07/08/2003. Retrieved from http://www.villagevoice.com/news/big-brother-gets-a-brain-6409852.

----------(2005). City snoop program returns?. *Defensetech*, 3/18/2005. Retrieved from http://defensetech.org/2005/03/18/city-snoop-program-returns/.

Scheeres, Julia (2002). Airport face scanner failed. *Wired Magazine*, 5/16/2002. Retrieved from http://archive.wired.com/politics/security/news/2002/05/52563.

Squires, P. (2010). Lessons from a surveillance culture. Paper prepared for, *Citizens, Cities and Video-Surveillance Programme. European Forum for Urban Safety*, May 2010. Retrieved from http://www.petersquires.net/research/cctv-surveillance/.

Trigaux, R. (2001). Cameras scanned fans for criminals. *St Petersburg Times*. 1/31/2001. Retrieved from http://www.sptimes.com/News/013101/TampaBay/Cameras_scanned_fans_.shtml.

Van der Ploeg, I. (1999). The illegal body: eurodac and the politics of biometric identification. *Ethics and Information Technology*, 1(4): 295-302.

Virilio, P. (1997). The overexposed city. In Leach, N. (ed.) *Rethinking architecture.* London: Routledge.

---------- (1994). *The vision machine*. Bloomington: Indiana University Press.

Yar, M. (2003). Panoptic power and the pathologisation of vision: critical reflections on the foucauldian thesis. *Surveillance and Society*, 1(3), 254-271.

[1] Foucault (2004).

[2] See for instance, Bousquet (1998); Butchart (1996); Cohen and Scull (1983); Cohen (1985); Gordon (1987 and 1990, 438-451); Horne and Maley (2014); Koskela (2003); Mann, Nolan and Wellman (2003); Marx (1988); Mathiesen (1980); Poster (1990).

[3] See Baumann (1992); Bogard (1996); Galloway (2004); Haggerty And Ericson (2000) especially 606-607; Haggerty (2006); Lianos

(2003); Lyon (1993); Lyon (2003); Mathiesen (1997); Newman (2009), 105; Yar (2003).

[4] Haggerty (2006) 27.

[5] It is important to note here that Foucault himself expanded beyond his analyses of Bentham's panoptic architecture. In his 1978 lectures, *Sécurité Territoire Population* (Foucault, 2004) Foucault described the effect of security mechanisms like vaccination campaigns on disciplinary regimes. In the history he tells here Foucault is clear that the security apparatus does not replace disciplinary power. Rather, in the same that educational apps depend on the classroom, security mechanisms depend on and modify disciplinary power by circumscribing and overlapping with it. For Foucault this development of security mechanisms occurs as a response to the problem of populations and as a further extension of biopolitical techniques of governance. See Deleuze's own acknowledgement of this in Deleuze (2003b), 229-240 and note 45 below.

[6] Foucault (1975) 234.

[7] The machinery of panopticism is such that even in the complete absence of the sovereign or her representatives, the design of the mechanism itself generates dissymmetry, disequilibrium and difference.

[8] "Whatever individual, taken almost at random, can make the machine function: in the absence of the director, his family, his entourage, his friends, his visitors, even his servants". Foucault (1975) 236.

[9] Note that the very design of the architecture, regardless of the actions of the detained within the cells, has *de-massifying* effects and, therefore, individualizing consequences for any inmate whether student, worker, convict or mad. See Foucault (1975) 234.

[10] See Lord (2015).

[11] As Glogster EDU's privacy policy states, this educational app vendor collects a vast amount of information on its young users: "name, address, email ... date of birth, gender, country, interests, hobbies, lifestyle choices, groups with whom they are affiliated (schools, companies), videos and/or pictures, private messages, bulletins or personal statements". The policy states that it regularly shares information with vendors developing, "consumer products,

telecom, financial, military, market research, entertainment, and educational services companies", Lord (2015)

[12] "It is, however, crucial to take that nuance into account because in current conditions *the majority of what one can call control does not focus on practices of constraint, nor on oppressing behaviour and expression, but on the organization and the contextualization of what is often intended or even desired by a sovereign subject*…This inversion is not neutral; it calls for the construction of a new framework of analytical premises. The most useful characteristic of such a framework should be to acknowledge that *the criterion for deciding what belongs or not to the sphere of control is neither the consciousness of the subject or the group involved, nor the will of those who produce the 'controlling' effect in question, but mainly the conditions that shape the interaction between those two parties*". Lianos (2003) 416.

[13] It is important to note that contemporary surveillance technologies are not merely technological innovations that have been discovered to carry along with them social impacts. These are technologies actively developed because they are seen as a viable response to particular political-economic pressures. Governments adopt automated surveillance systems because they wish to limit or eliminate labor costs where possible. At the same time the same governments must appear actively engaged in reducing crime and creating safe zones for consumption. The political need to appear engaged in reducing crime acts as a major motive for deploying these technologies. On the other hand, the narrowing profit margins for companies drive companies to develop these technologies in an effort to successfully target niche consumers.

[14] See section iii below.

[15] Or, *automated optical imaging*. See below, section v.

[16] See Lyon (2003) 20-22 and 26-28; also, Los (2006) 77-79.

[17] Bowker and Star (1999) even argue that software is better understood as, "frozen organizational and policy discourse". (135)

[18] Lyon (2003) 15.

[19] See Baumann (2013).

[20] As Lyon (2003) describes: "The coding is crucial because the codes are supposed to contain the means of prediction…The codes form sets of protocols that help to alter the everyday experience of surveillance". (24)

[21] Most surveillance strategies in wealthier societies depend increasingly upon high speed computing. Searchable databases coupled with remote networking capabilities have allowed surveillance to extend from monitoring fixed subjects from fixed locations to mobile positioning where both surveillants and surveilled can be simultaneously in motion. Thus, two elements have become key to the effectiveness of contemporary surveillance: information processing and reliable communication networks. It is important to note that this technology does not just 'happen'. Consider for a moment the shift to the importance of CCTV in Europe, North America and Asia in dense urban environments and the link up of these to a growing range of locational devices that not only situate data subjects in a fixed space but also while on the move. See Lyon (2003) 16.

[22] Emily Gilbert (2010) explains: "[for face recognition surveillance] there is a great variability in rates of recognition on the basis of age, gender, and race. Faces that deviate from the standard (such as the faces of visible minorities) are more likely to trigger a mechanized and/or human response. Thus a standard is inbuilt to which normalcy gets affixed, while those whose facial characteristics differ are implicitly construed as abnormal and targeted as potential 'risky subjects'. These processes are especially hard to detect when the underlying decision-making (the decision threshold policy) is obscured, and the comprehension of its mechanisms is in the hands of only a small number of experts. Moreover, the experts themselves perpetuate biases in the management of the data as a 'security continuum' is drawn across multiple and disparate realms – such as crime, unemployment and immigration – by security professionals. Inbuilt biases may by themselves be minimal, but they can become multiplied and magnified as they become tied to other practices and spread across multiple networks". (234) See also G. Agamben's (2004) argument in his letter to *Le Monde*, "*Non au tatouage biopolitique*".

[23] Bowker and Star (1999) explain that the biases expressed by particular systems are not always intentional: "Some are the [result of the] tyrannies of inertia – red tape – rather than explicit public policies. Others are the quiet victories of infrastructure builders inscribing their politics into the systems. Still others are almost accidental – systems that become so complex that no one person

and no one organization can predict or administer good policy". (50)

[24] See, "You are being tracked: how license plate readers are being used to track American's movements". ACLU (2013)

[25] As Norris and Armstrong (1999) show being young, male and black in Britain ensures a higher rate of scrutiny by Britain's 4 to 6 million street-mounted CCTV cameras.

[26] Introna and Wood (2004).

[27] Introna and Wood (2004) describe two main categories of facial recognition algorithm – image template algorithms and geometry feature-based algorithms. Both operate according to the principle of reduction: "In order to be efficient in processing and storage the actual face image gets reduced to a numerical representation (as small as 84 bytes or 84 characters in the case of FaceIt)". (186) Because of the way these algorithms reduce facial features in order to form a biometric facial signature of the person in question bias is unavoidable.

[28] See Introna and Wood (2004).

[29] See Introna and Wood (2004).

[30] Introna and Wood (2004) 184-194. Also Gilbert (2010).

[31] Introna and Wood (2004) 184-194.

[32] In this way Haggerty and Ericson (2000, 619-620) speak meaningfully of the disappearance of disappearance.

[33] See Haggerty and Ericson (2000).

[34]"*Post-scriptum sur les sociétés de contrôle*" was originally published in *Futur antérieur*, (1) Spring 1990. It was later reprinted in the collection, *Pourparlers* (2003) 240-244.

[35] For Deleuze, a panoptic space like the prison is also a kind of surveillant assemblage but one that attempts to close itself off to connections with outside spaces. As Bogard (2006) describes it: "A machinic assemblage joins or separates diverse material flows. For example, the prison, as Foucault sees it, is a territorial machine that works by enclosing and partitioning space, segregating bodies, or again, by connecting them together by larger, functional ensembles, coordinating their corrective flows, and so on". (104)

[36] "Dans les sociétés de contrôle, au contraire, l'essentiel n'est plus une signature ni un nombre, mais un chiffre : le chiffre est un mot de passe, tandis que les sociétés disciplinaires sont réglées par des mots d'ordre (aussi bien du point de vue de l'intégration que de la

résistance). Le langage numérique du contrôle est fait de chiffres, qui marquent l'accès à l'information, ou le rejet. On ne se trouve plus devant le couple masse-individu. Les individus sont devenus des «dividuels», et les masses, des échantillons, des données, des marchés ou des «banques»", Deleuze (2003a) 241. See also Deleuze (2003b).

[37] Societies of control function through mechanisms that report the positioning of any element within an open environment at any given instant. For Deleuze, coding is crucial to this shift because codes are at the basis of predictive systems. These systems anticipate events (like crimes), conditions (like ebola), and behaviors (like smart phone consumption) that have yet to occur. Further, the old world of surveillance dependent on the layout of the city has now been transformed by what Virilio calls *audio-visual protocols*. (Virilio, 1997, 383) For Virilio the key to contemporary urban surveillance is *pro*spection, or vision in advance (Virilio. 1989). The function of this kind of surveillance is not to discipline bodies but to sort them, subjecting them to regular events of interruption and re-direction as they pass through the surveillance context.

[38] As Bogard (2006) states: "In its more advanced forms, it [the surveillant assemblage] is like a 'pre-recording' machine that can capture performances 'in advance' (in the same sense clones are like pre-recorded life forms, or profiles are pre-recorded statuses or identities". (107)

[39] *Striation* refers to the process of introducing breaks and divisions into otherwise free flowing phenomenon. See Deleuze and Guattari (1987) 385.

[40] As an *assemblage,* surveillance environments constitute a collection of objects – cameras, fingerprint scanners, databases, tip hotlines, facial recognition algorithms etc – whose unity comes from how these different objects function together to shape a field of unified effects. For Deleuze and Guattari any discrete assemblage is itself composed of multiple assemblages, which, in turn, are multiple. See Patton (1994) 158.

[41] These processes operate from scattered centers of calculation, which, for Haggerty and Ericson (2000) include sites like forensic laboratories, statistical institutions, police stations, financial institutions, and corporate and military headquarters; as they describe them: "In these sites the information derived from flows

of the surveillant assemblage are reassembled and scrutinized in the hope of developing strategies of governance, commerce and control". (613)

[42] For the surveillance assemblage, the human body is increasingly then also a cyborg, or a flesh-technology-information amalgam. See Haraway (1991) chapter 18. As a collection of processing devices, the surveillant assemblage renders digitally 'visible' a host of flows from auditory, olfactory, tactile, chemical, visual, ultraviolet and informational inputs.

[43] See Haggerty and Ericson (2000) and Haggerty (2006).

[44] Haggerty and Ericson (2000) 612. See also Bogard (2006); Galloway (2004) 13; Lyon (2003) 22-24 and (2006) 86-89; and note 3 above.

[45] As Deleuze (2003b) states in his 1990 interview with T. Negri: "[Foucault] was actually one of the first to say that we're moving away from disciplinary societies, we've already left them behind. We're moving toward control societies that no longer operate by confining people but through continuous control and instant communication. Burroughs was the first to address this. People are of course constantly talking about prisons, schools, hospitals: the institutions are breaking down. But they're breaking down because they're fighting a losing battle. New kinds of punishment, education, healthcare are being stealthily introduced. Open hospitals and teams providing home care have been around for some time. One can envisage education becoming less and less a closed site differentiated from the workspace as another closed site, but both disappearing and giving way to frightful continual training, to continual monitoring of worker-schoolchildren or bureaucrat-students. They try to present this as a reform of the school system, but it is really its dismantling. In a control-based system nothing is left alone for long". (244)

[46] As Newman (2009) states: "Control techniques are used not so much to identify a particular individual, but rather to identify a future risk and to attach this risk to certain types of individuals". (106)

[47] Introna and Wood (2004) 182.

[48] "[CCTV] was oversold – by successive governments – as the answer to crime problems. Few seeking a share of the available funding saw it as necessary to demonstrate CCTV's

effectiveness…Yet it was rarely obvious why CCTV was the best response to crime in particular circumstances" (Gill and Spriggs, 2005, 116).

[49] "It would be easy to conclude from the information presented in this report that CCTV is not effective: the majority of the schemes evaluated did not reduce crime and even where there was a reduction this was mostly not due to CCTV; nor did CCTV schemes make people feel safer, much less change their behaviour." (Gill and Spriggs, 2005, 115). See also Home Office/ACPO (2007) 4-5 and Squires (2010).

[50] For instance, a distinct shift can be detected in claims made about Atlanta's, *Operation Shield*, a surveillance network composed of both private and public sector cameras monitored by a video integration center (VIC). In 2011 David Wilkinson, President of the public-private Atlanta police foundation claimed Atlanta's video integration center (VIC) would integrate both public and private security cameras into a network that, "will use software that can identify suspicious activity and guide officers right to the scene of a crime as it's occurring. In effect, the software will multiply the eyes and ears of the five to seven people per shift who will initially monitor video footage around the clock". (Garner, 2011) However, two years later expectations have clearly been lowered. While Atlanta's surveillance network has grown from 500 private-public cameras in 2011 to 1200 in 2013 operators no longer claim that the network will prevent crime much less record criminal acts as they occur: "As Lieutenant Leanne Browning points out, instead of spotting crime as it happens, the VIC is more useful for discovering details after the fact". Where claims were made in 2011 that software would direct cameras with 'Gun Spotter' software to cue up to the sound of gunshots now the goal of developers is to eventually coordinate camera coverage with incoming 911 calls. Still, the city is committed to spending $350,000 yearly to place cameras at $13,000 apiece to provide coverage of Atlanta's parks by 2016. Developer's claim that "soon 10000 cameras will cover the city" but given that the system began in 2007 and by 2013 had only managed to network 1200 cameras this claim seems another example of vendor hyperbole driving expenditure of mostly public money on technologies whose effectiveness does not match expectations. Especially disturbing is the reciprocity agreements

between at least some private security firms and the Atlanta police department that allow private security access to the APD cameras. See Blau (2012) and Rehagen (2013).

[51] Chicago is an especially important case to consider because Chicago's private camera system is the most extensive, expensive and integrated one in the United States. As of 2013 its $60 million network linked some 22,000 private and public cameras. However, the effectiveness of the system continues to be questioned. One study (La Vigne, 2011) showed the cameras brought decreases in certain kinds of crime in one neighborhood (Humboldt Park) with no noticeable effect on crime rates in another (West Garfield Park). Another study suggested the cameras do not influence certain kinds of violent crime at all or register only a modest reduction when they are first introduced with no further gains registering with increasing saturation of the area with cameras (Reese, 2011). However, as Chapman (2010) argues: "Chicago police say the cameras have produced 4,000 arrests since 2006. That sounds like a lot, but it works out to only about 1 in 200 arrests." This kind of argument is especially important given the cost of the Chicago system and the constant calls from government officials to increasing camera coverage throughout the city.

[52] See Trigaux (2001), Canedy (2001), Scheeres (2002) and ACLU (2002).

[53] Assuming that there were at least some sought-for individuals among the populations under surveillance and that the systems failed to trigger an alert on any person of interest over the time of their deployment then the chances are considerable that the system issued also *false negatives* as well as false positives.

[54] Virilio (1994, 60) states: "Once we are removed from the realm of direct or indirect observation of synthetic images created *by the machine for the machine*, instrumental virtual images will be for us the equivalent of what a foreigner's mental pictures already represent: an enigma. Having no graphic or videographic outputs, the automatic-perception prosthesis will function like a kind of mechanized imaginary from which, this time, we would be totally excluded".

[55] Also known as machine vision.

[56] Though a human interface is still needed for set up and the customization of the light patterns given context and the product. Nor should it seem a limitation of this technology that these examples focus on vision systems as deployed currently in factory line settings since, for Foucault, panoptic logics initially structured factory environments. Further, these automated visioning systems are literally replacing work that until very, very recently could only be performed manually by people. See Bachelor and Waltz (2001).

[57] See Bachelor and Waltz (2001) 201-203. Also consider the interface on *Baxter* by Rethink Robotics at Carr (2013).

[58] Refers to a small television camera tube. The image is formed on a transparent electrode coated with photoconductive material.

[59] See Colucci (2010).

[60] As DARPA's (2003) *Pre-Solicitation Notice* explains, the CTS program, "explores concepts, develops algorithms, and delivers systems for utilizing large numbers (1000s) of cameras to provide the close in sensing needed for military operations in urban terrain. Combat Zones that See will advance the state-of-the-art for multiple-camera video tracking, to the point where expected track lengths reach city-sized distances. Trajectories and appearance information resulting from these tracks are the key elements to performing higher-level inference motion pattern analysis on video-derived information. Combat Zones That See will assemble the video understanding, motion pattern analysis, and sensing strategies into coherent systems suited to Urban Combat and Force Protection". As the then head of DARPA, Tony Tether (Schactman, 2005), argued before the Senate Armed Services Committee: "*We need a network, or web, of sensors to better map a city and the activities in it, including inside buildings, to sort adversaries and their equipment from civilians and their equipment, including in crowds, and to spot snipers, suicide bombers, or IEDs (improvised explosive devices). We need to watch a great variety of things, activities, and people over a wide area and have great resolution available when we need it. And this is not just a matter of more and better sensors, but just as important, the systems needed to make actionable intelligence out of all the data". Tether's observations could be applied easily both to cities in North America and cities in battlefields in the Middle East. See also Schachtman (2003) and Graham (2006a), (2006b) and (2010).*

[61] Developers and institutional consumers of these technologies describe them as if destinies come built into the technology and to a certain extent the analyses of Deleuze seem to accept that the technology functions as advertised. Again, CCTV certainly does not operate in Chicago, Atlanta, or the UK as intended. Also, in the midst of the camps of the planners, designers and implementers of these systems there is considerable disagreement on what these systems are capable of actually accomplishing, once deployed, in the real world. Thus, considerable conflicts exist among the branches of the armed forces about the efficacy of CTS with the Army and Marines expressing particular skepticism about its use-value for real world combat environments.

[62] For Stephen Graham (2006a, 256) systems like CTS operate by sorting citizen from Others and by sorting legitimate citizens from those who may behave as Others. Such machinery of surveillance originates in the demand to conduct an ongoing, limitless kind of social sorting that would sort out, "…citizens who are deemed to warrant value and full protection of citizenship and those deemed threatening as real or potential sources of 'terrorism'". (Graham, 2006a, 260). See also, Graham (2010), 199-223.