M. Strano, H. Hrachovec, F. Sudweeks and C. Ess (eds). Proceedings Cultural Attitudes Towards Technology and Communication 2012, Murdoch University, Australia, 25-37.

THE GAZA STRIP AS PANOPTICON AND PANSPECTRON: THE DISCIPLINING AND PUNISHING OF A SOCIETY

MICHAEL DAHAN
Sapir College, Israel
dahanm@gmail.com

Abstract. This paper explores the different yet complementary aspects of the panopticon and the panspectron using the case study of the Israeli controlled Palestinian territory, the Gaza Strip. Beginning with a brief theoretical discussion of the concept of panopticon and panspectron expanding on the existing literature, the paper moves on to discuss the implementation of panoptical and panspectral technologies and practices in the Gaza Strip and situates these within a larger framework of control of the Palestinian population under Israeli occupation, and discusses seepage of these surveillance technologies into Israeli society proper and beyond into the international arena.

1. From Panopticon to Panspectron

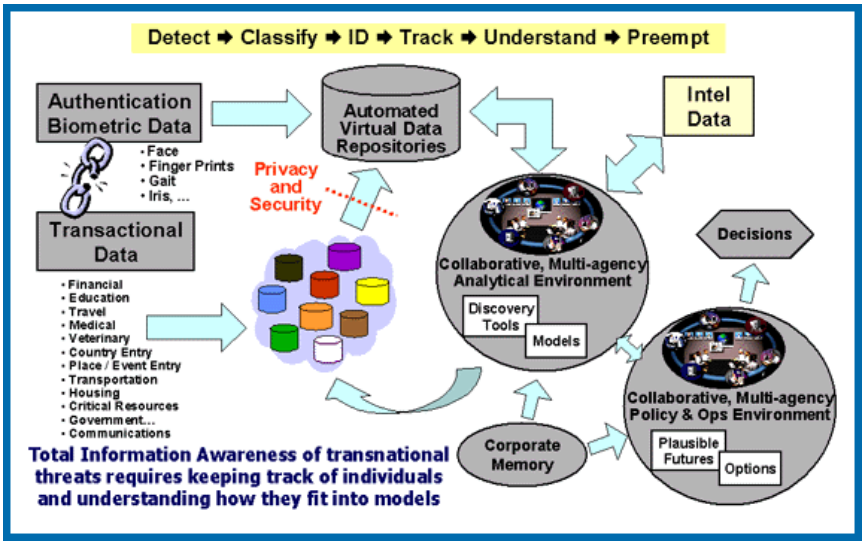
In the late 18th Century, English philosopher and social theorist Jeremy Bentham designed an institutional building which he called the Panopticon. Bentham saw the design as "a new mode of obtaining power of mind over mind in a quantity hitherto without example". (Bentham, 1787/1995, p.i). Essentially, the architecture of the building allowed surveillance of people at all times without the objects of surveillance knowing that they were being observed at any given moment. The constant observation or gaze of the authorities would then serve to affect and change behavior. Since then, Bentham's panopticon has served as a model for the construction of prisons, and has become a metaphor for surveillance and "big brother". Michel Foucault in Discipline and Punish: The Birth of the Prison (1975/1977) later continues the exploration of the panopticon from an institutional perspective noting that the role of the panopticon is "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" (p.199). The following passage from Orwell's novel 1984 summarizes succinctly the effect of panopticon:

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time… You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every moment scrutinized (Orwell in Sclove 2000, p.22).

Manuel DeLanda (1991; Palmas, 2011), describes how the National Security Agency in the US was putting together a surveillance system that he calls 'the panspectron'. In contrast to the original panoptic architectures and social and organizational constructs of Bentham and Foucault, the panspectron monitors a wider segment of frequencies of the electromagnetic spectrum, if not the entire spectrum. In other words, the panspectron not only registers that which is visible to the human eye but also radio, radar, microwaves, cellular communication, and so on:

> Instead of positioning some human bodies around a central sensor, a multiplicity of sensors is deployed around all bodies: its antenna farms, spy satellites and cable-traffic intercepts feed into its computers all the information that can be gathered. This is then processed through a series of 'filters' or key-word watch-lists. The Panspectron does not merely select certain bodies and certain (visual) data about them. Rather, it compiles information about all at the same time, using computers to select the segments of data relevant to its surveillance tasks (DeLanda, 1991, p.206).

While the panopticon is concerned primarily with individual surveillance and control, the panspectron is about mass surveillance and control: everything and everyone is observed all the time. The goal here to being to monitor as completely as possible what Floridi (2002) terms the "infosphere". In many ways the Total Information Awareness (TIA) program instituted by the Pentagon in the aftermath of 9/11 is panspectral in nature. While the program was discontinued in 2003, many components of the program continue to be developed under different names. An infographic provided by the now defunct US Information Awareness Office provides us with a possible conceptualization of the panspectron:



It is important to note here that panoptical and panspectral technologies are not mutually exclusive and can and often do coexist in given situations. Sandra Braman (2006) goes further and uses the concept of the panspectron to describe, among other aspects, the ability of what she terms the "informational state" to expand its sovereignty and control beyond its borders through technology. She observes (2006) that "in the panopticon environment the subject knows that the watcher is there, in the panspectron environment one may be completely unaware [and often is] that information is being collected". Braman provides examples of panspectral technology usage at US border crossings, and by the TSA in non US airports as examples of the extension of sovereignty beyond national borders. Other countries use social networking sites to check arrivals at airports (see Fassahi, 2009). Indeed, even so called democratic and even "liberating" technology, such as Web 2.0 implementations credited with fueling the Arab Spring, have at their core panoptical and panspectral aspects, which we contribute freely in the framework of what Albrechtslund (2008) calls participatory surveillance:

> With the transition from a panopticon to a panspectron environment, the production of open information not only provides support for communities but also contributes to surveillance (Braman, 2006).

Or as Andrejevic remarks:

> The participatory injunction of the interactive revolution extends monitoring techniques from the cloistered offices of the Pentagon to the everyday spaces of our homes and offices, from law enforcement and espionage to dating, parenting, and social life. In an era in which everyone is to be considered potentially suspect, we are invited to become spies – for our own good (Andrejevic, 2005, p.494).

Indeed, intelligence organizations thrive on the myriad mapping of social relationships which can be used to gain information and leverage against a specific subject. In particular they are concerned with the mapping of social networks of political activists and what they term subversive elements. Social networking platforms provide these organizations with this information voluntarily. This was indeed the case in most of the demonstrations in the Middle East over the past year, and prior to this in Iran during the protests against what was seen as election fraud on part of the ruling party. The same technologies that allowed for the dissemination of information and political mobilization also allow the intelligence and security organizations in these countries to track and arrest activists[1]. In the West Bank and Gaza information gathered by the security services allowed the Palestinian Authority and Hamas, respectively, to arrest organizers of demonstrations thus quelling demonstrations and dissent[2].

While Tawil-Souri (2011), Zureik et al. (2010), and others have probed and exposed the differing aspects of panoptical control implemented by Israel in the Gaza Strip, as well as the West Bank, this paper seeks to expand the existing analysis by

---

[1] See Open Net Initiative for country reports detailing net surveillance at http://opennet.net/

[2] Information gleaned from anonymous interviews with members of Palestinian IT Association (PITA).

addressing additional dimensions of control, including panspectral control hereto unaddressed, as well as seepage into Israeli society and beyond of technologies of control tested and used in the West Bank and Gaza, such as the proposed biometric identity system, facial recognition systems, expansion of CCTV implementation and the internal use of surveillance balloons (previously used only at borders with Israel) and drones which allow security authorities to control all communications including internet access within a given area, as well as collect information and mount attacks via the remote controlled aerial drones. Once these technologies become normalized within a civilian context they then become the basis for policy. For example, behavioral and ethnic profiling, initially developed by Israel for aviation security (Whitaker, 2011) has now become the gold standard in airports around the world. Furthermore, technologies and methods developed in the course of control of the Gaza Strip are selectively implemented within Israeli society and beyond in the so called "war on terror", (Gordon, 2010) or for social control, and are then exported abroad. Indeed, in the wake of September 11 and the demand for homeland security technology (Rygiel, 2008, p.88), Israel has become a “24 hour showroom… Turning war into a brand asset” (Klein, 2007). Some have ventured so far as to suggest that the recent (February-March 2012) violence in Gaza was instigated by Israel in order to showcase its “Iron Dome” technology – marketing it both to the public (to ease fears) in preparation for a possible war with Iran, and to the US and other countries as a solution for missile attacks. The process would seem to be reinforced by the dialectical relationship between the tool or technological solution, its uses and policy that is adopted in light of its apparent success. This is usually achieved with little public debate. Surveillance technologies thus seep from the battlefield to civilian use, providing the state with significant control of the civilian population, often under the pretense of the “war on terror” and the need for democracies to defend themselves from internal and external threats. Webster (1999) notes, states tend to exploit the application of new technology, particularly surveillance technology in order to strengthen their own legitimacy and deepen their control both internally and externally. Indeed it would seem that Israel expresses its sovereignty primarily as control.

2. Gaza as Panopticon *and* Panspectron

> One of the most powerful strategies of imperial dominance is that of surveillance, or observation, because it implies a viewer with an elevated vantage point, it suggests the power to process and understand that which is seen, and it objectifies and interpellates the colonized subject in a way that fixes its identity in relation to the surveyor… The imperial gaze defines the identity of the subject, objectifies it within the identifying system of power relations and confirms its subalterneity and powerlessness (Ashcroft, Griffiths and Tiffin 1998, p.226, quoted in Zureik et al.).

The Gaza Strip lies on the Eastern coast of the Mediterranean Sea. It is bordered on the southwest by Egypt, and by Israel on the east and the north. The Strip itself is 41

km long, and between 6 and 12 kilometers wide. Its total area is 360 square kilometers and contains a population of approximately 1.7 million, a majority of which are refugees. It is one of the most densely populated areas in the world. The Gaza Strip is physically separated from the rest of the Palestinian Territories in the West Bank. Following the Israeli unilateral disengagement from the Gaza Strip in 2005, including the withdrawal of settlers and military, control of the Gaza Strip was assumed by the Palestinian Authority. In 2006 the Hamas won a majority of votes in the Gaza Strip and formed a national unity government with Fatah. In 2007 violence broke out between the Fatah and Hamas factions after which Hamas seized control of the Gaza Strip and replaced Fatah officials with its own. Following Hamas control of the Gaza Strip, Israel instituted (with Egyptian assistance) a complete land closure and naval blockade of the Gaza Strip. This is also supported by Palestinian Monetary Authority which provides foreign (i.e. Israeli and American oversight) of financial transfers[3]. This has resulted in the Gaza Strip essentially becoming the world's largest open air prison. The only effective way in or out of the Gaza Strip, whether people or commodities, is through a series of hundreds of underground tunnels connecting the Gaza Strip to Egypt. In fact, the only physical dimension of Gaza that Israel does not control is these tunnels, and the tunnels are the only way that Gazans can escape the imperial gaze. The tunnels also serve as a form of resistance to and egress from, the panoptical and panspectral gaze. Thus, in many ways Gaza resembles the dystopic visions expressed in cyberpunk literature, and is reminiscent of such movies as the 1981 *Escape from New York.* As Gary Fields explains:

> enclosure is thus the application of force to land by groups with territorial ambitions who mobilize the institutional power of law and the material power of architecture to reorder patterns of land ownership, use, and circulation and reorganize socioeconomic life and demography in a place (Fields, 2010, p.66).

Control of Gaza by the Hamas, as well as the closure forced Israel to invest in technological solutions for surveillance and control as they no longer had access to the extensive network of collaborators and informants which comprised Israel's human intelligence within the Gaza Strip. As Sa'adi (2005) notes, Israel has relied on networks of informants within the occupied territories for decades. These physical networks were often supported by technological means. As Lyons (2001) points out, an analysis of surveillance is grounded on the fact that it is "real" people watching over others, but the new quality of surveillance lies in the fact that this "embodiment" lessens and is transferred to computers and other technological systems. This is clearly reflected in the evolution of the strategies of surveillance in the Gaza Strip. More so, Gaza has become the testing ground for new panoptical and panspectral technology in a hereto unprecedented form.

Among the technological mechanisms of surveillance and control in the Gaza Strip one may find the use of biometric identity cards, Israeli access to Palestinian census data, almost complete access to and control of the telecommunication infrastructure in

[3] See Palestinian National Anti Money Laundering Committee at: http://www.ffu.ps/

the Gaza Strip (Tawil-Souri 2011), the ability to track individuals via cell phone, large surveillance zeppelins (see photo below) which monitor the entire electromagnetic spectrum and which can usurp control of these from Palestinian operators (for instance sending text messages to subscribers targeting different demographics) as well as optical surveillance, unarmed UAVs for surveillance and targeting, armed UAVs that carry out targeted assassinations, facial recognition technology (used for identifying individuals in large crowds of people – negating the possibility of public anonymity), remote controlled and robotic machine gun towers guarding the border that are capable of identifying a target and opening fire automatically – without human intervention. These technologies as well as the more recent "Iron Dome" (which targets missiles and is capable of destroying them in mid air) are being tested by the US army for defense of its bases in hostile areas like Afghanistan.

Surveillance zeppelin permanently positioned above the Gaza Strip

I recently had the opportunity to view some of these technologies first hand at the Erez Crossing between Gaza and Israel[4]. The crossing has undergone a massive restructuring in recent years, and now resembles more than anything else, an airline terminal or ultra modern border crossing (see below). Originally conceived as the primary land crossing and entry point into Israel (prior to the 2007 closure) the structure is quite impressive and was intended to make the crossing seem more humane while at the same time providing maximum security to Israeli supervisors.

Beyond exploring the biometric identity system I was also sensitive to the architecture of the structure. Pedestrian flows within the terminal are directed in such a way as to prevent any direct contact between Israeli security and the Palestinians. Security officers (many of the crossings and checkpoints in the occupied territories have been privatized), patrol on gangways situated between the ceiling and the ground floor. Interior design attempts to hide varying aspects of control, including control of the flow of people within the terminal. The architecture eventually guides prospective entrants to a series of identification cubicles. Each cubicle has a biometric identity system composed of a biometric facial recognition system which compares the individual to the biometric facial data on his or her ID card and the biometric database maintained by Israel, a fingerprint system which reads all ten fingerprints (fingerprints are one of the

[4] The tour was arranged informally and technically illegal. As a result my ability to document, particularly photograph, was severely limited.

first "scientific" forms of identification and were first used by the British colonial administration in India), and finally a biometric palm reader (the same palm reading system is used as a voluntary ID system at Ben Gurion airport to facilitate entry and exit for registered Israeli citizens). The prospective entrant must be identified by all components in order to gain entry. In addition to this each biometric identity card is also equipped with a unique RFID chip which allows for tracking within the terminal and beyond. Different aspects of the system can be seen in the photo below (one caveat regarding the photo: there is no physical presence in the cubicle with the Palestinian prospective entrant. The photo was provided by the ministry of defense).

It is not only the geographical and technological closure that comprise the panopticon and panspectron that is the Gaza Strip. Then Chief of Staff Moshe Ya'alon described one of the goals of the "operation defensive shield" in 2002 during the second Intifada as being to "etch the consciousness" of the Palestinians in such a way and with such force that they would not even consider resistance, i.e. "resistance is futile". This is a recurring theme in Israeli technological hegemony and in exerting its sovereignty and maybe found in the logic behind the stuxnet virus directed against Iranian nuclear facilities. Apparently a joint US/Israel cyber attack, beyond damage to the facilities one of the implications of its success is to suggest "we can get hold of you anywhere" or as Zurawski (2005) notes "we know where you live". Perhaps most representative of this tactic was the targeted assassination by Israel in 1996 of Yahya Ayyash, a bomb maker for Hamas and one of the leaders of the Iz Adin al Qassam Brigade. He was killed by a small amount of explosive hidden in his cell phone. When he answered and his identity established the charge was detonated remotely, killing him instantly. Beyond the obvious purpose of assassination, the method used served to send a message of technological superiority to those challenging Israel. The "etching" was to be achieved by both military means and the use of great force ("shock and awe"), but also through technological control. This echoes Foucault's "mind over mind" (1995:206). Indeed one of the main targets of information gathering during the operation by Israeli forces dealt with Palestinian census data and the wholesale rifling and destruction of the Palestinian Central Bureau of Statistics data files. The goal of "etching the consciousness" of the enemy has become an integral part of the "Operational Art" of the IDF (Rappaport, 2010), and was practiced during the Second Lebanon War as well, with Israel using massive firepower directed at infrastructures as well as commandeering of cellular networks and television stations. Text messages were sent directly to citizens' cell phones during defensive shield, the Gaza incursions and the Second Lebanon War (Rappaport, 2010).

3. Seepage of Panoptical and Panspectral Technologies

Israel controls 70% of the market in aerial drones (UAVs) (used for observation and attack) and is a leader in the development of border surveillance technologies, such as sensors, aviation security systems and protocols, fences, electro-optical equipment, and robotic gun systems (Denes, 2011; Gordon, Zureik, & Kloostermann, 2010). In addition, a macro level view of the hi-tech sector in Israel shows an inordinate amount of research and development in the field of surveillance and data collection as well computer security systems. Earlier research has shown that the roots of the Israeli hi tech sector are in Military Intelligence (particularly one specific signals intelligence unit, Unit 8200) and the defense industries. The "special relations" between Israel and The US provide Israel with access to large markets in North America, Europe, Azerbaijan and Eastern Europe, China, India, and until recently, Turkey.

The clearest seepage of control technologies developed in the context of the occupation into Israel proper is the proposed use of biometric ID cards for Israeli citizens. Israel has long used a system of differentiated ID cards to distinguish between Jews and non Jews, citizens and residents of Israel, and citizens and residents of the

occupied territories. These ID cards are color coded: Blue for Israeli citizens and Arab residents (but not citizens) of East Jerusalem, orange for Palestinian residents of the West Bank and Gaza. The ID cards also note ethnic/religious affiliation, and the ID numbers themselves are coded so as to reflect this information. In fact this system of identification is perhaps the oldest example of social sorting in Israel. ones identity status, whether citizen or resident, Israeli or Palestinian determines your freedom to travel (both within Israel and abroad), ones ability to marry and to receive social benefits, as well as ones ability to find employment.

In 2008 the Interior Ministry, the government entity responsible for administering the national registry, began to advance what was initially called "Smart ID", but later became known as biometric ID card. According to then-Interior Minister, Meir Sheetrit, biometric cards would assist in 'uprooting crime, foiling terror attacks and identifying victims' (Ilan, 2009)[5]. While the project has been delayed due to public pressure and is currently classified as a non mandatory pilot, individuals arrested during this pilot period have had their biometric data taken and added to the database. It is expected that after the two year trial registration with the database will be mandatory and lack to comply will be punishable by law. Israel has also pressured Palestinians to create their own biometric database and hand it over to Israel in the interest of "biometrization"[6].

In 2007 the Israeli parliament approved a bill dubbed the "Big Brother" law, permitting police to establish a massive database or search engine based on telecom information. The new law allows police to request a judge's warrant to obtain communications data from a database that includes telephone numbers, names and real time location of mobile phone subscribers, hard serial numbers of mobile phones, and maps of cellular antenna locations. Under certain conditions high ranking police officers can obtain this information without prior judicial consent. The Knesset rejected requests to grant the police authority to receive lists of internet addresses in Israel (Ilan, 2007). As a result, eavesdropping by the police and security services increased tenfold (Ilan, 2008). In addition, secret police units have been conducting surveillance of Israeli citizens (including political activists) using a myriad of methods (Zarchin, 2009).

Furthermore, a secret appendix exists in all telecommunication licenses issued by the Ministry of Communication. All communications providers are required to be licensed by law. In the license is a secret appendix or codicil which explicitly demands that telecommunications companies hand over, by request of the security services any information related to voice calls and text messages, location information and usage patterns. There is little or no evidence of Internet surveillance or deep packet inspection

---

[5] For a comprehensive discussion of the issues as voiced in the Israeli press, see: Ilan, Shahar (2009/03/15) 'Plan to introduce biometric IDs stirs privacy debate', *Haaretz*. http://www.haaretz.com/hasen/spages/1070793.html;
Ilan, Shahar (2008/05/18) 'Police wiretaps climb sharply in peripheral areas', *Haaretz*. http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=984365
Ilan, Shahar (2007/12/18) 'Knesset okays establishment of "Big Brother" database for police'. http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=935812&contrassID=0 &subContrassID=0

[6] See Hass, Amira (2009/11/25) 'Voyeurism', *Haaretz*. http://www.haaretz.com/hasen/spages/1130498.html

in Israel proper, nor is their much in the Palestinian Territories: the majority of blockages are related to sites with sexual content. It is worthy to note here though that Israel controls almost all the bandwidth in the occupied territories as well as much of the electromagnetic spectrum – obstensively for security reasons (World Bank 2008a, 2008b).

Another technology that has found its way into use by the police is facial recognition technology. Initially developed and tested by the military in order to identify both Israeli and Palestinian protestors during demonstrations against the wall in Bili'n and Ne'alin villages near Ramallah[7]. This technology is now being used by the police to identify protestors within Israel proper (cross referencing with the national register), and is being implemented at airports and border crossings. The surveillance zeppelin has also made a number of appearances in Israel, usually during visits of heads of state but also during large public protests. These surveillance zeppelins provide the operators with control over telecommunications in a certain radius, including the Internet. All of these technologies as well as additional surveillance technologies form the backbone of an extensive exportation of surveillance technologies abroad in the framework of homeland security. Over 300 Israeli companies are actively involved in the homeland security sector. For an informed discussion on the political economy of Israel's home land security sector see Neve Gordon (Gordon, 2010). Analysis of Israel's UAV industry is provided by Nick Denes (2010).

Israel has adopted a screening and surveillance model that is openly and routinely used. Israeli behavioral profiling methods, Whitaker (2011) suggests, are arguably necessary for a state fixated on the importance of ever-improving security measures. At the same time the author problematizes the racially-based deployment and development of such security protocols.

In addition to being a significant developer and exporter of surveillance equipment, the Israel's military/security industry is also a world leader in the perfection of surveillance methodologies and techniques (Morley, 2012). Using the airport as a case study, Whitaker examines screening procedures that were developed and implemented by Israel and its security services (see Kloosterman 2010). Similarly, Pfeffer (2009) analyses the development of racial profiling as an anti-terrorist and security measure initially used by Israel's security agencies within airports. This method is credited with virtually eliminating all terrorist attacks in Israeli airports since the 1970s. 'Many Israelis have no problems with this [strategy]', Pfeffer asserts. 'Let the Muslims suffer for the sins of their brothers they say. But those of us who like to think of ourselves as liberal humanists find it all too easy to ignore the sight of entire families having their luggage rummaged through in front of the entire terminal while we are waved through'. In this sense, privileged Jewish Israeli's become complacent, even comfortable with the extent to which the security apparatus provides them protection, while simultaneously disenfranchising and oppressing others. It is not hard to imagine similar sentiments being expressed in the US in light of behavioral and racial profiling. Much of Whitaker's argument can be summarized as follows:

[7] I first became aware of during interviews conducted with IDF reservists. I have been unable to receive confirmation by the IDF, Ministry of Defense, Ministry of Internal Security nor has this been reported in the press.

> Looked at strictly as a security measure, Israeli passenger profiling has a number of strengths. Even its critics acknowledge that *it works*. However, looking at it simply as a socially and politically neutral security technique misses a great deal that is critical to grasping the significance of passenger profiling in its specific Israeli context (2011, p.383, emphasis in original).

4. Conclusion

While many of the technologies discussed in the framework of "seepage" can be understood in terms of Giddens' (1985) (and echoed by Lyon, 2001) proposed connection between citizenship rights and surveillance (based in turn on Marshall's (1973) typology of political, social and economic rights in the modern state) i.e the policing or security aspect of surveillance and the role of surveillance in the provision of rights, the changes in approaches to political thinking in a post 9/11 reality coupled with restrictions on political liberties, (primarily in the US, Israel, Russia, the UK and France) the rise of populism and the general backlash against democracy – often precursors to authoritarianism – brings us one step closer to the panspectron within modern and currently democratic societies. Indeed, it would seem that in recent years, in response to threats of terrorism and economic instability, liberal democracies, with the aid of technologies of surveillance and control, are rapidly shedding liberal characteristics and moving toward a form of democracy where the state has a great deal of potential control of the population. As Giddens notes, "aspects of totalitarian rule are a threat" in all advanced societies precisely because surveillance is "maximized in the modern state" (Giddens, 1985, p.310). The case of the Gaza Strip, unique as both an open air prison and as a live example of panoptical and panspectral technologies is informative at two levels: the attempt by Israel to use these technologies in order to gain complete and total panspectral control in a Deleuzian sense (and to punish when deemed necessary by Israel) while serving as a testing ground for similar technologies to be implemented in the framework of advanced societies. One only need to look at the narratives of control surrounding immigration issues in the US and Europe, the unprecedented use of surveillance technologies (particularly CCTV, vehicle tracking in large cities, the "participatory surveillance" of social media, the proliferation of location based mobile technology and the use of police drones) to consider that the future may not bode well.

References

Andrejevic, M. (2005). "The work of watching one another: Lateral surveillance, risk, and governance," *Surveillance & Society*, 2(4): 479–497, and at http://www.surveillance-and-society.org/articles2(4)/lateral.pdf.

Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance, *First Monday*, 13(3). Retrieved from http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949

Bentham, J. (1995). *The Panopticon Writings*. Ed. Miran Bozovic (pp.29-95). London: Verso.

Braman, S. (2006). Tactical Memory: The Politics of Openness in the Construction of Memory. *First Monday*, 11(7): 1-21.
DeLanda, M. (1991). *War in the Age of Intelligent Machines*. New York: Zone.
Denes, N. (2011) From tanks to wheelchairs: Unmanned aerial vehicles, Zionist battlefield experiments, and the transparence of the civilian. In E. Zureik, D. Lyon and Y. Abu-Laban (eds) *Surveillance and control in Israel/Palestine: Population, Territory and Power*. London: Routledge.
Fassahi, F. (2009). Iranian Crackdown Goes Global. *Wall Street Journal*, 3 December. http://online.wsj.com/article/SB125978649644673331.html
Fields, G. (2010). Landscaping Palestine: Reflections of Enclosure in a Historical Mirror. *International Journal of Middle East Studies* 42:63-82.
Floridi, L. (2002). Information Ethics: An Environmental Approach to the Digital Divide, *Philosophy in the Contemporary World*, 9(1), 39-45.
Foucault, M. (1975/1977). Discipline *and Punish: The Birth of the Prison*, New York: Random House.
Giddens, A. (1985). *The Nation State and Violence: Volume Two of a Contemporary Critique of Historical Materialism*. Cambridge: Polity Press.
Gordon, N. (2010). Israel's Emergence as a Homeland Security Capital. In E. Zureik, D. Lyon and Y. Abu Laban (eds.) *Surveillance and Control in Israel/Palestine* (pp. 199-218). London: Routledge.
Halabi, Usama (2011). Legal analysis and critique of some surveillance methods used by Israel. In E. Zureik, D. Lyon & Y. Abu-Laban (eds) *Surveillance and Control in Israel/Palestine* (pp. 199-218). London: Routledge.
Ilan, Shahar (2009/03/15). Plan to introduce biometric IDs stirs privacy debate, *Haaretz*. http://www.haaretz.com/hasen/spages/1070793.html
Ilan, Shahar (2008/05/18). Police wiretaps climb sharply in peripheral areas, *Haaretz*.http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=984365
Ilan, Shahar (2007/12/18). Knesset okays establishment of "Big Brother" database for police'. http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=935812&contrassID=0&subContrassID=0
Isin, Engin F. (2004). The neurotic citizen, *Citizenship Studies*, 8(3): 217-235.
Jeffay, Nathan (2009/08/12). Israel poised to pass national I.D. database law, *The Jewish Daily*. http://www.forward.com/articles/112033/ (accessed March 9, 2010).
Klein, N. (2007). How War has Turned into a Brand, *The Guardian*, June 16. http://www.guardian.co.uk/commentisfree/2007/jun/16/israel.comment1
Kloosterman, K. (2010/03/16). Israel's Top 10 airport security technologies, *The Matzav Network*. http://matzav.com/israels-top-10-airport-security-technologies
Lis, J. (2009/12/16) 'MKs pass controversial bill to set up biometric database', *Haaretz*. http://www.haaretz.com/hasen/spages/1133498.html
Loewenstein, J. (2006). Identity and movement control in the OPT, *Forced Migration*, 26: 24-26.
Lyon, D. (2001). *Surveillance Society: Monitoring Every Day Life*. Philadephia, PA: Open University Press.
Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.
Marshall, T. H. (1973). *Class, Citizenship, and Social Development*. Wesport, CT.: Greenwood.
Morley, J. (2012). Israel's Drone Dominance, *Salon.com*. http://www.salon.com/2012/05/15/israels_drone_dominance/singleton/
OpenNet Initiative (2009). Internet filtering in Gaza and the West Bank. http://opennet.net/research/profiles/gazawestbank
Oren, A. (2010/02/17) 'Under surveillance / Big Brother changes everything', *Haaretz*. http://www.haaretz.com/hasen/spages/1150121.html
Palmås, K. 2011. Predicting What You'll Do Tomorrow: Panspectric Surveillance and the contemporary Corporation. *Surveillance & Society* 8(3): 338-354.

Pfeffer, A. (2009/11/01). In Israel, racial profiling doesn't warrant debate, or apologies. *Haaretz*. http://www.haaretz.com/hasen/spages/1141297.html

Rappaport, A. (2010). *Lessons for the IDF from the Second Lebanon War*, Begin Sadat Center for Strategic Studies, Paper number 85, Bar Ilan University, Israel. Hebrew.

Rygiel, K. (2008). Citizenship as Government: Disciplining Populations Post-9/11. In J. Leatherman (ed.). *Discipline and Punishment in World Politics* (pp.85-110). New York: Palgrave and MacMillan.

Sclove, R. (2000). Privacy and Power: Computer Databases and Metaphors of Information Privacy. Unpublished Manuscript.

Tawil-Souri, H. (2011). The Hi-Tech Enclosure of Gaza. In Larudee, M. (ed). *Gaza-Palestine: Out of the Margins*. Ibrahim Abu-Lughod Institute of International Studies Birzeit University, Ramallah.

Webster, F. (1999). *Theories of the Information Society: Second Edition.* Routledge.

Whitaker, R. (2011). Behavioural profiling in Israel aviation security as a tool for social control. In E. Zureik, D. Lyon & Y. Abu-Laban (eds), *Surveillance and control in Israel/Palestine: Population, Territory and Power*. London: Routledge.

World Bank (2008a). West Bank and Gaza Telecommunications Sector Note: Introducing competition in the Palestinian Telecommunications Sector. http://web.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/03/20/000333037_20080320052257/Rendered/PDF/429870WP0GZ0Te10Box327342B01PUBLIC1.pdf

World Bank (2008b). Introducing competition in the Palestinian Telecommunications Sector'. http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/MENAEXT/WESTBANKGAZAEXTN/0,,contentMDK:21698862~menuPK:294386~pagePK:141137~piPK:141127~theSitePK:294365,00.html

Yoaz, Y. (2007/09/25). Secret clause lets Shin Bet get data from cell phone firms, Haaretz.com. http://www.haaretz.com/hasen/spages/906489.html

Zarchin, Tomer (2009/10/15). Secret police unit monitoring Israeli citizens, Haaretz, http://www.haaretz.com/hasen/spages/1120635.html

Zurawski, N. (2005). 'I Know Where You Live!' Aspects of Watching, Surveillance and Social Control in a Conflict Zone (Northern Ireland). *Surveillance & Society* 2(4): 498-512

Zureik, E, Lyon, D, and Abu-Laban, Y. (Eds.) (2010). *Surveillance and Control in Israel/Palestine*. London: Routledge.