SURVEILLANCE-FICTION OR HIGHER POLICING?

By : ***Jean-Paul Brodeur***
Stéphane Leman-Langlois

K. Haggerty et R. Ericson, *The New Politics of Surveillance and Visibility*, Toronto, University of Toronto Press, 171-198.

INTRODUCTION

In past and recent work, one of us tried to articulate a distinction between high and low policing (Brodeur, 1983, 1992, 2000 and 2003). This distinction was initially formulated in France in the seventeenth century and elaborated upon by Napoleon's minister for policing, Joseph Fouché. In simple terms, low policing consists in law enforcement and high policing in political surveillance (L'Heuillet, 2001). More precisely, high policing was defined by four features: (1) it was absorbent policing, hoarding all-encompassing intelligence on socio-political trends, while making parsimonious use of this information in the actual prosecution of individuals, neutralized only when deemed strictly necessary; (2) it conflated legislative, judiciary and executive or administrative powers, the police magistrate enjoying all three; (3) its goal was the preservation of the political regime ("the State") and not the protection of civil society; (4) to this end, it made extensive use of informants that infiltrated all walks of society. These features traditionally were combined within a police paradigm where the protection of the political *status quo* was the primary goal of policing and where furthermore the interests of the regime were not seen to be coterminous with the interest of civil society.

Although the most potent symbol of political surveillance is now Orwell's Big Brother, high policing was not initially a totalitarian paradigm, even if it was not constrained by rules of accountability (Brodeur, 1983). Indeed, as Brodeur tried to argue initially, high policing cancelled out the notion of police deviance. This point was neatly encapsulated by a member of the French *Assemblée nationale*, who recently delivered a report on the accountability of the French security services. He advocated that they be granted a large amount of unfettered discretion according to the principle that in the field of national security "the rights of the State supersede the rule of law" ("*Les droits de l'État commandent à lÉtat de* droit;" France, *Assemblée nationale*, 2002: 3)

In the 1983 paper on high and low policing, it was argued that the coming years would witness the rise of high policing and Brodeur later attempted to show in a paper entitled "Cops and Spooks" (Brodeur, 2000), published before the tragic events of September 2001, that high and low policing agencies shared an increasing common ground, albeit with various degrees of discomfort. Since 9-11, this conclusion cannot be doubted for obvious reasons reaching much beyond my limited gifts of foresight, or anybody's for that matter. This paper is divided in three parts. First, we give a selective account of major developments in political surveillance that occurred in Canada and the US, after September 2001. Second, we review the features of high policing, as described in 1983, asking to what extent they still apply in the present context. In a concluding section, we discuss a new set of features of political surveillance.

DEVELOPMENTS IN POLITICAL SURVEILLANCE

In such a short essay, we cannot give an account, however brief, of all the developments in political surveillance after September 2001. In Canada, the main legislation enacted after 9-11 – Bill C-36 – has over 180 pages and was followed by other legislation. In the US, the USA Patriot Act of 2001 has 10 titles and 182 sections. To this must also be added the numerous provisions of the Cyber Security Enhancement Act passed on November 19, 2002, by the US Senate as an Amendment to the Homeland Security Act, which brought together 22 agencies and some 170 000 personnel. Such massive complexity is in direct contradiction with Habermas' argument that the cornerstone of a democratic society is the possibility of public debate. Not only were these laws adopted without any informed public debate, but it is dubious that the legislators themselves were fully aware of what they were voting on. A recent feature in *The New York Times* has shown that when the Senate passed the 80 billion USD bill to pay for the impending war in Iraq, it didn't notice that it was also voting for dozens of other pork-barrel projects, among which were 10 million USD to a research station at the South Pole that had had a hard winter and 3.3 million USD to fix a leaky dam in Vermont – not to mention allowing the Border Patrol to accept donations of body armour for dogs (Firestone, 2003). A sprinkle of increases of the surveillance power of various agencies is as undetectable, in such huge bills of legislation, as pork-barrel.

In this wealth of developments, we shall focus on the Communications Security Establishment in Canada and in the Total Information Awareness project in the US, which appear to us among the most significant. The latter project was recently rechristened *Terrorism* Information Awareness, because its reach into privacy was disturbing for the US public, the civil libertarians and even the political class.

Canada and the Communications Security Establishment (CSE)

Although it was created under its present name in 1975, the CSE's history began earlier in 1941, when a secretive unit called the Canadian Examination Unit (XU) was created for the purpose of interception and decipherment of the enemy's electronic communications. The crucial development occurred in 1947, with the signing of the UKUSA treaty that brought together the US, the UK, Australia, New Zealand and Canada into an alliance devoted to the interception of radio communications, known today under the acronyms of COMINT (communications intelligence) and SIGINT (signal intelligence), as opposed to HUMINT (human intelligence) which is collected by persons rather than by machines. In Canada, the Canadian Security Intelligence Service (CSIS) is the main HUMINT agency. In the UKUSA treaty, the US was designated as the first party to the agreement and the other four nations as second parties (Bamford, 1982: 399). It is this partnership that is the object of much criticism in Europe, under the name of ECHELON. The European Parliament has commissioned reports to investigate ECHELON.

Like its US counterpart the National Security Agency, the CSE was not created by legislation but by a decree of the executive (Order-in-Council PC 1975-95). The agency, which is part of the Department of National Defence, has two components: the first one is comprised of civilian experts that perform various tasks ranging from cryptology to intelligence analysis and covert operations (Frost and Gratton, 1994); the second one is manned by the military personnel that operate the Canadian Forces Supplementary Radio System

(CFSRS). Originally, the CFSRS was to monitor communications in the Soviet Arctic, using technology provided by the US government (for instance on the Island of Ellesmere).

The CSE is highly secretive and its mandate was spelled out in full only in 1997, in the first report of the CSE Commissioner, the civilian watchdog of the agency (CSE Commissioner, 1997: 5-6). Initially, the CSE had a twin mandate. As Canada's cryptology agency, it collects and analyses foreign radio, radar and other electronic emissions and through the provision of SIGINT it contributes to the government's foreign intelligence program. The CSE also manages Canada's Information Technology Program (ITS), which provides technical advice, guidance and various other services in support of government telecommunications security. The CSE thus operates in both an offensive and a protective capacity. It always emphasized that its offensive capacity was exclusively directed at foreign communications and that Canadians were not targeted. Although put in doubt earlier (Sallot, 1984), this claim has been so far vindicated by the CSE Commissioner, since he has started to report in 1997.

This may now change. Following the 9-11 attacks in the US, Canada enacted Bill C-36, which increased in various ways the surveillance powers of the police. Moreover, embedded in C-36 was a little noticed Trojan horse: Bill C-36 actually provided the CSE with its enabling legislation, surreptitiously introduced as a sub-part of part V of the National Defence Act, which bears on military justice and has no relationship at all with SIGINT. In all its reports, the CSE Commissioner had emphasized that such legislation be the object of a wide public debate. This is precisely what did not happen, the enabling legislation being adopted under pressure, with few if even any amendments. Yet such a debate was crucial, especially since the enabling legislation added a new and controversial component to the CSE mandate. On top of its foreign intelligence and ITS duties, the CSE is now also "to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties" (subsection 273.64 (1) c). The federal agencies referred to are the Royal Canadian Mounted Police (RCMP), the Customs and CSIS, among others.

The CSE's involvement in policing may not be problematic in certain respects, as when it would provide help to other agencies in deciphering lawfully intercepted communications. However, it may itself assist federal law enforcement and security agencies in the interception of private communications. According to Canadian law, such interception requires judicial authorization that is granted on the basis of an affidavit explaining the reasons for the interception, its instruments and its target(s). One of us (Brodeur) explicitly asked the personnel of the CSE Commissioner's office whether such an affidavit would mention the CSE's assistance in performing an interception. The answer was that this was indeed a good question ("you are right on the money") but, for reasons of national security, no answer could be given. There are other grey areas surrounding the CSE's implication in policing and law enforcement.

This is all the more troubling because of the massive investment of Western governments in SIGINT. In the US, the budget of the NSA is much bigger that the CIA's. Because of the fact that CSE personnel are recruited among civilians and military, it is difficult to get the true figures in relation to personnel and budget. In a comparative study of the CSE and of CSIS' respective manpower and budgets in the years preceding 2001, one of us found that the CSE was spared the drastic cuts that affected CSIS and that overall, its budget was probably higher than that of CSIS (Brodeur, 2003: 231). This tentative finding was in fact confirmed after 9-11. The Canadian government injected an additional 47 million dollars (Canadian) in the protection of its national security shortly after September 2001. The CSE was granted the greatest portion of this money, 37 million as compared to 10 million for CSIS.

In a speech given on January 30th, 2003, on the occasion of the release of his annual report for 2002-2003, the Privacy Commissioner of Canada issued a dire and pressing warning that the federal government was on the way of destroying essential rights to privacy, with important consequences on the freedoms enjoyed by Canadians (Privacy Commissioner of Canada, 2003). His call should be heard, but perhaps in a somewhat weaker, yet more crucial, sense than he meant it. It may be too late to protect privacy from state and non state intrusion: all that is left would be to strengthen the means to guarantee that the data collected on us are valid, that is not riddled with gross mistakes as it is generally found when personal data are assessed in quality control exercises (Laudon, 1986). In April 2003, the Canadian government announced that a much criticized data-bank on air travellers would be de-nominalized, a protection of privacy expedient that is also used in the US (Buzzetti, 2003a). What this means is that data is stored on patterns of activities and on transactions, while the name of the persons engaging into these activities is provisory put in brackets. The name of a particular individual is sought only when a threatening pattern of behaviour has been discovered. We shall return to this topic at a later stage.

The US and the Total Information Awareness project

Following 9-11, the US Congress conducted a joint House and Senate inquiry into the failure of the intelligence community to prevent the attacks against the World Trade Center and the Pentagon (US, Congress, 2002). The joint committee's report is long on general findings and recommendations but short on details. However, the Vice Chairman of the Senate Select Committee on Intelligence, Senator Richard C. Shelby, issued his own report, which is tantamount to shock treatment in reality therapy on the efficiency of the US national security apparatus in counterterrorism (Shelby, 2002). Senator Shelby was not the only one to blow the whistle, as a scathing memo written by FBI agent Coleen Rowley has shown.

Senator Shelby documents two series of shortcomings which, even when we take into account the benefit of hindsight, appear grievous.

– Two individuals, Khalid Al-Mihdhar and Nawaf Al-Hazmi, were spotted by the Malaysian security service attending an Al Qaeda meeting in Kuala Lumpur, where the terrorist operative that had organized the attacks against USS Cole, in Yemen, was also present. This information was passed on to the CIA. There exists in the US a surveillance program – TIPOFF – according to which the name of suspicious individuals trying to enter the US or to get a visa is given to immigration and visa issuing authorities that then block the entry of the suspects in the US. For unclear reasons, the CIA failed to use TIPOFF until it was too late, although both individuals entered and left the US on several occasions and finally settled under their own name in San Diego, where they took flying lessons. The CIA also refused to share with the FBI its knowledge of the presence of these two terrorists on US soil. Both were aboard the plane that exploded against the Pentagon.

– When Zacharias Moussaoui was arrested while he was taking flying lessons in the US, the legal separation between criminal prosecution and foreign intelligence prevented the FBI agents investigating him to get a warrant to access his computer (where the name of Mohammad Atta, the chief organizer of 9-11 was later to be found). In order to get such a warrant, they were advised that they had to connect him to a known terrorist organization and tried in vain to link him to Chechen terrorists. When they finally obtained a warrant, 9-11 had already occurred.

These two cases are of particular interest for the clues they provide regarding the two key metaphors guiding the reform of political surveillance in the US.

– The first one is "connecting the dots." In these cases, the dots were not connected for two reasons: (1) the lack of horizontal integration, which kept the various services from sharing their information, and (2) the dismal quality of intelligence analysis.

– The second one is "the wall" separating foreign security intelligence from its use in domestic law enforcement, thus preventing any kind of vertical integration between intelligence and field operations. This divorce is forcefully decried by Senator Shelby: "Intelligence analysts would doubtless make poor policemen, and it has become very clear that policemen make poor intelligence analysts" (Shelby, 2002: 62).

Shelby's judgement does not seem to leave much ground for appeal: "The Bureau's failures leading up to September 11 thus suggest the possibility that *no* internal FBI reorganization will prove able to effect real reform" (Shelby, 2002: 70, emphasis in text). It is in this context that computerized surveillance, such as it is embodied in the Total Information Awareness (TIA) program, seems to offer an alternative to human fallibility:

> I mention TIA here at some length because it represents, in my view, precisely the kind of innovative, "out of the box" thinking…which Americans have a right to *expect* from their Intelligence Community in the wake of a devastating surprise that left 3,000 of their countrymen dead. It is unfortunate that thinking of this sort is most obvious in the Defense Department rather than among the Intelligence Community leaders… (Shelby, 2002: 43, emphasis in text).

Before we describe TIA in further detail, we should make clear that funding for the program has recently been cancelled by the Senate (by the Department of Defence Appropriations Act of 2004, section 8120). Yet it remains a powerful example of a general trend in policing and surveillance. And as we will discuss later, the disappearance of TIA by no means implies the disappearance of the tactics and technologies it was developing. Note for instance that the newly created Department of Homeland Security (DHS) has its own “advanced projects” department (the Homeland Security Advanced Projects Agency, HSARPA), which it will provide with 500 million USD a year to develop technologies similar to the TIA program.

TIA was a strategy initially developed within the Pentagon by the Information Awareness Office (IAO), one of two data analysis projects developed by the Defense Advanced Research Projects Agency (DARPA; the other program is the Information Exploitation Office (IXO) and focuses on real time battlefield operations). At its inception the IAO was headed by Vice-admiral John Poindexter, who was acquitted on appeal for his alleged role in the Irangate scandal. At the core of the TIA project is a computerized Big Brother that is, paradoxically, claimed to reconcile all-encompassing surveillance with privacy rights. This reconciliation would rest on a crucial difference between surveillance as exercised by humans (HUMINT) and surveillance as exercised by machines, that is, computers, which we shall call COMPUTINT. When a police officer or an intelligence agent listens to intercepted communications, he or she knows that only a small part of the information thus collected can be used in actual proceedings against the suspect. However, these listeners cannot erase from their memory all that they learn on the intimate life of the suspect, which can be potentially used for blackmail purposes, even if it was not initially relevant to the investigation at hand. This invasion of intimate life is felt to be particularly obnoxious by those submitted to surveillance (Plenel, 1997). As they are machines, computers, it is claimed, can be programmed to retrieve from a surveillance project only what is strictly relevant to its lawful purpose and not to keep on file what is unrelated to that purpose. In contradistinction from HUMINT, COMPUTINT can be made strictly selective. To a significant degree, the IAO’s version of privacy is an offspring of this conception of the properties of computers. Needless to say, this claim rests upon a great deal of confidence in the computers’ programmers.

TIA had three components. The first component was analytical. Ninety percent of all terrorist incidents that have occurred were submitted to detailed analysis in order to extract, from their minute description*, patterns* that may be predictive of terrorist behaviour. To give a simple example, such a pattern may be (1) paying in cash (2) for plane tickets (3) purchased in a small or medium size airport, (4) leaving the date of the return trip open. The second component of TIA, which we shall call *transactional*, consisted in the computerized monitoring of daily transactions occurring in the US. This monitoring would be quite extensive as it would involve mining financial, educational, travel, medical, veterinary, country entry, place/event entry, transportation, housing, critical resources, government and communications data (note that this information was removed from the IAO web site even before the death of the project). The third and last component was to perform the actual *identification* of individuals that triggered an alert by engaging into a recognized behavioural pattern. The computer would then go through authentication biometric data and the operators of the system could try to intercept the individual(s) for questioning before they have a chance for further action. Even if there was pervasive monitoring and data-mining undertaken by the second component of the system, it was argued that privacy would not be intruded upon, as the computer would trigger an alert only if a person’s behaviour matched a previously established threatening pattern. Thus, the data in the transactional component would have been, to all practical purposes, de-nominalized, as was the case with the previously mentioned Canadian data-bank on travellers.

There are some additional features of TIA on which we want to briefly comment. First, most of it was heavily "outsourced," the realisation of the project resting in the hands of private firms. Raytheon, Syntek Technologies (Mr. Pointdexter was its vice-chairman), Booz Allen, Hamilton Inc. (whose vice-president, Mr. Mike McConnell, previously chaired the NSA), Hicks and Associates, Microsoft, Intel and Veridian Corporation were important participants. New firms kept appearing at each visit of the now defunct IAO Web site. Second, the marketing of high technology is not entirely governed by a principle of *adequacy* (whether the purchased technology will aptly do the job) but also by a principle of *availability*. Although there is generally a balance between these two principles, which on the whole is favourable to adequacy, the question of availability becomes prominent in crisis situations where *one must do with* what is to be found on the market, because of urgency. There is no better example of this than the use of automated translation software. TIA was to make use of automatic translation software – Translingual Information Detection, Extraction and Summarization (TIDES) and BABYLON, a version of TIDES that can be used on handheld computers – because the US intelligence community was faulted for its lack of foreign language skills. The problem with automatic translation is that it doesn't work beyond giving a vague impression of the content of a message (the Canadian government stopped subsidizing the *Université de Montréal*, which devoted diehard efforts to automatic translation research, when it failed to develop software that would translate weather forecast bulletins, which use the simplest of language, between French and English). Still, the use of automated translation technology was expanded in the last version of TIA (May 2003) by the integration of GALE (Global Autonomous Language Exploitation) a new software program for mining data in verbal and written communications in foreign languages. Note that translation software projects all survived the demise of the IAO/TIA and were simply put under the responsibility of other entities. There are many other examples of computer technology integrated to the system with little quality control. Such wrong-headed can-do obstinacy may result in impeding efficiency rather than enhancing it, when one is facing real life terrorists.

TIA died while still in development. It was first planned to be ready by 2005-2006, *before* the US Congress decided, in the spring of 2003, to limit funding and to authorize only a limited application to foreign nationals. In September of 2003, the Senate gave it the coup de grace and axed all and any TIA projects having anything to do with data mining. Yet, despite the early death of TIA, the concept it embodies – electronic profiling of individuals against a background of behaviour-predictive transactional patterns – is gaining ground. In March 2003, the US Congress – while cutting funds to the TIA – granted authority to the federal Transportation Security Administration for developing a system for screening passengers which is a clone of TIA applied to air travellers. It is called Computer Assisted Passenger Prescreening System (CAPPS) and is already under fire from privacy advocates. It is currently under review by the U.S. General Accounting Office, which will report on it in February 2004.

So the TIA spirit remains alive and well. In many quarters, including the already mentioned Transportation Security Administration, who is cutting down on the number of armed air marshals who were supposed to be assigned to flights in the U.S., data mining and analysis is seen as the answer to most security problems, in spite of ongoing public relations nightmares. Those nightmares previously prompted the transformation of *Total* Information Awareness to *Terrorism* Information awareness, and *Bio-Surveillance*, one of the TIA sub-projects, to *BioAlirt* (Bio-event Advanced Leading Indicator Recognition Technology). It also caused the original IAO logo, which included an all-seeing eye and the motto, *scientia est potentia*, to vanish from the publications of the office. These minor adjustments were not sufficient to offset the last scandal of the IAO, in the summer of 2003: the FutureMap project, which invited investors to trade in terrorism futures on the internet in order to exploit the claimed predictive powers of markets. This last straw caused John Poindexter to resign from office and Senate to cancel all funding.

It should be evident, then, that the demise of the IAO and its TIA was due to a monumental lack of political acumen – or in fact basic cultural awareness – on the part of those responsible, and not to a loss of confidence in the technology. In fact that confidence is stronger than ever and even DARPA remains involved with projects such as LifeLog and "Combat Zones that See" (CTS), which could erase the boundary between battlefield awareness and policing, on an extremely large scale. Some of the TIA sub-programs may have been taken over by the Army Intelligence and Security Command (INSCOM), who was an active testing and development partner for TIA (this should be clarified with the February 2004 report of the Technology and Privacy Advisory Committee). The CIA has recently commissioned Systems Research and Development to develop a new data mining tool named Anonymous Entity Resolution. Not to mention that private enterprises and universities who built the TIA technologies are unlikely to simply scrap them and the research already done on the system. Finally, and once again in startling ignorance of popular culture, a program dubbed MATRIX – like the blockbusting series of movies depicting a totalitarian, machine-controlled dystopian fantasy – is implementing the TIA principle at state level with funding from the Department of Justice (MATRIX is a contrived acronym for Multistate Anti-TeRrorism Information eXchange). Note that MATRIX is operated by private (profit and non-profit) entities, and that its central server is located on private premises (those of Seisint, inc., a computer technology firm founded by a known drug smuggler).

HIGH AND LOW POLICING REVISITED

We shall now review the four features that were originally attributed to high policing in order to see if they fit the analysis of political surveillance undertaken in the first part of this paper. This review will also provide us with an occasion to probe deeper into the meaning of these traits.

Absorbent policing

Absorbent policing is a mixture of profligacy and of parsimony. On the prodigal side, it is characterized by the accumulation of intelligence that purports to be all-compassing, as if the whole informational content of civil society was sucked into the State's data banks. Mustering the resources of information technology, initiatives like TIA would appear to be the true accomplishment of this part of the program of high policing. Furthermore, the root metaphor of "connecting the dots" underlines the structural nature of security intelligence: intelligence is not a mere pile of data but a network of cross-references.

On the stingy side, high policing was not only retentive in the sense that it hoarded information, but it was also restrained in its use if this information in *public* prosecutions of individuals. It was *quiet* policing that apparently distanced surveillance from punishment. There were historical reasons for this restraint, as the targets of high policing were often members of the aristocracy that threatened the Sovereign's power and who were powerful enough in their own right to make the government cautious in dealing with them. It was also progressively discovered that quiet policing was cost effective, because it instilled dread into the whole populace through the stealthy character of its operation. The efficiency of the *Panopticon* lies not in watching all but in having all chillingly believe that they are exposed to constant surveillance.

This second feature of high policing is more controversial in the present context, where the alleged "wall" between security intelligence and law enforcement is perceived as a major impediment to efficient protection. There does not seem to be a consensus on how to solve this problem. A first strategy is to break through the wall. It is clearly exemplified in Canada by legally directing this most remote of our intelligence services – the CSE – to assist federal law enforcement agencies. In the US, it is expected that police forces will have prime access to most data mining tools, as they do now with MATRIX. According to this strategy, high and low policing will merge, the capacity of law enforcement agencies for high and "intelligence-led" (as this last concept is now being floated in the UK) policing being enhanced.

On the other hand, it seems that some critics, like Senator Shelby, have nearly given up on the police as intelligence workers and that the "tyranny of the casefile" (Shelby, 2002: 62) and that their shortcomings in the sharing and analysis of the wealth of information available to them are insuperable. In this second script, not only would the divorce between high and low policing be consummated, but it may be that the lead agencies for high policing would fall under the military rather than the intelligence community. This development could have nefarious consequences. As the present skirmishes between the CIA and the Pentagon are showing, the military may be even more autistic than the intelligence community in its appraisal of situations (Risen, 2003).

The accumulation of powers

The high police magistrate was not simply a powerful officer of the executive (the eyes of the Sovereign), but he also presided over a police tribunal that could adjudicate justice and order punishment and, finally, he enjoyed wide regulatory powers that made law for most professions and occupations. This feature of high policing is, it would seem, the most remote from the present reality, because of the formal distinction between legislative, judiciary and executive powers which has been embodied in our laws since at least the time of Montesquieu.

Yet in practice, it is more or less recognized, since Jerome Skolnick's classic essay (1966), that police provide "justice without trial" and make law on the streets. This observation was made in reference to all policing and had no specific relationship to high policing. But today high policing is being reshaped by a massive call for the prevention of terrorism, and in this context, one should speak of pre-emption rather than prevention, since what is involved are proactive efforts to minimize risk as much as is brutally possible within a partisan interpretation of the precautionary principle. (1) In this respect, police may not yet enjoy legislative powers, but they are certainly endowed, by executive *fiat*, with the power to circumvent the rules of due process and to name confidentially those who should be arraigned. Preventive detention of persons considered to be a threat to US security bears witness to this fact, although its extent is not publicly disclosed. (2) All incarceration amounts to punishment, regardless of whether it is preventive or repressive – preventive incarceration is actually considered as more punitive by the courts, because of its indeterminate character – and should be inflicted upon an individual only after a judicial hearing. This applies even more to the death penalty, which is the ultimate sanction. Yet both incarceration and exceptionally, the death penalty, are applied within the scope of high policing, as they are explicitly authorized by the executive, the first as preventive detention and the second as political assassination. With the imposition of incarceration and *a fortiori* the death penalty, high policing is thus becoming a substitute for proceedings normally conducted by the judiciary. (3) Needless to say, the police exercise all their policing powers in respect to pre-emption. It would then seem that under a “state of pre-emption”, high policing actually exerts powers which are normally separated.

Preservation of the regime vs. the protection of society

This, as we argued at the beginning of this chapter, is the hallmark of high policing: it is entirely devoted to the preservation of a political regime. It rests upon an identification of the internal opponent with the foreign enemy, against whom the State has to be protected. The partial recycling of national security agencies into “economic security” is now the latest incarnation of this trait. Historically, “enemy of the state” was an extensible category that included leaders from the aristocracy claiming a right to the throne and their partisans; all were perfunctorily said to be supported by a foreign power. It also included religious opponents, who were also suspected of being agents of countries that had officially established the religion that was banned in their own country (e.g., French Protestants were seen as potential agents of England, Holland and Denmark). It also included political and social agitators that could drive mobs to riot, for example, in the case of famine, and notorious criminals who enjoyed some popularity in their defiance of the State’s rule. These were not believed to have been recruited by a foreign power, but their actions were seen as either destabilizing or as an intolerable blemish of the majesty of the sovereign.

A similar state of mind, which tended to assimilate all internal dissidence to the great Communist threat, was pervasive during the Cold war and during the U.S. war against Vietnam; it culminated with President Nixon being obsessed with “enemies” during his presidency. The abuses of high policing were finally investigated by the Church and Pike commissions, who published influential reports (respectively US Congress, 1976 and US Congress, 1977). However, it would seem that the 9-11 attacks resulted in bridging whatever gap may have remained in the post-Cold war days between the State and U.S. citizens, and in generating a new consensus of fear. In respect to its present engagement in counter-terrorism, high policing cannot be considered as affording protection to the regime, as opposed to the citizens of the U.S. or other countries. Instead, high policing is now apparently devoted to the protection of the citizens, whose interests are assumed to coincide with the State's. It would then seem that the hallmark feature of high policing – taking side for State against civil society, does not apply as well in the aftermath of 9-11.

There is an undeniable part of truth in this insight. But upon closer examination the situation shows far more complexity. We shall now argue that the former blurring of the line between violent terrorism and political dissidence is being reinvented as a progressive erosion of the boundary separating the nationals of a country from foreigners on its territory. The consequences of this undermining of the basis of citizenship are portentous in respect to surveillance.

Following the Church and Pike inquiries, measures were taken to curb police covert operations, such as the FBI's notorious COINTELPRO, particularly when they targeted U.S. citizens. Similar measures were taken in Canada in the early 1980s, following the Keable (Québec, 1981) and the McDonald (Canada, 1981) inquiries: when CSIS was created in 1984, its agents were strictly defined as intelligence officers and not granted policing (peace officer) powers, in order to bar them from engaging in "disruptive tactics."

The most wide-ranging reform, however, was to limit political surveillance to foreigners. As we have seen, the Canadian CSE is forbidden to intercept private communications if either the originator or the recipient of the communication is a Canadian citizen or a legal resident of Canada. In the U.S., the Foreign Intelligence Surveillance Act (FISA) was enacted in 1978. It was the main statute governing political surveillance in the US but its content was in this respect ambiguous, as it is shown if Senator Shelby's report, of which we shall quote two excerpts.

> Much of the blame for the dysfunctional nature of pre-September 11 law enforcement agencies/Intelligence Community coordination can be traced to a series of misconceptions and mythologies that grew up in connection with the implementation of *domestic* intelligence surveillance (and physical searches) under the Foreign Intelligence surveillance act (FISA) (Shelby, 2002: 46, our emphasis).
>
> The Bureau disseminated extraordinarily few intelligence reports before September 11, 2001, even with respect to what is arguably its *most unique and powerful domestic intelligence tool*: collection under the Foreign Intelligence Surveillance Act (FISA) (Shelby, 2002: 66-67, our emphasis).

What is rather striking in those quotations is the assertion that the main statutory instrument for *domestic* political surveillance comes from an act that granted authority for the purpose of collecting of *foreign* intelligence information. This foreign intelligence orientation was strengthened by US case law stating that "the "primary" purpose of the requested surveillance or search be the collection of *foreign* intelligence (Shelby, 2002: 53). To all practical purposes, FISA made it difficult to target US citizens, who were protected by FISA "minimization rules" for handling information on US citizens or lawful permanent residents. Political surveillance was apparently directed against foreign nationals. Even in this last case, the law limited surveillance to the collection of intelligence, divorced from the bringing up of criminal charges against a FISA target of surveillance (Shelby: 52-53, see note 105). The ultimate result of such legislation – be it in the US or Canada– and of its narrow interpretation was to harden the dichotomy between nationals of a country and foreigners on its territory. Such a result can have dire consequences in times like ours, when the distinction between natives and aliens is blurred by strong migratory pressures that make it difficult to decide unambiguously who is a stranger in the land and who is not. In March 2003, in the midst of the war against Iraq, the FBI sought to interview between 3 000 and 11 000 Iraqi-born people, focusing on Iraqi immigrants rather than Iraqi-Americans. However, it seems that in the actual interviews, this distinction was not always followed (Hakim and Madigan, 2003).

The USA Patriot Act of 2001 lifted the limitations that jurisprudence had set to political surveillance under FISA. This law had provided for years that the primary purpose of political surveillance undertaken under its authority had to be intelligence collection. Section 218 of the Patriot Act stated that:

> Sections 104(a) (7) (B) and section 303(a) (7) (B) (50 U.S.C. 1804(a) (7) (B) and 1823 (a) (7) (B)) of the Foreign Intelligence Act of 1978 are each amended by striking “the purpose” and inserting “a significant purpose”.

The upshot of that amendment, which was later to be confirmed by the newly created FISA Court of Review, is that the amended FISA statute permits surveillance and physical searches even for undertakings that are primarily intended to result in the criminal prosecution of individuals, provided that a “significant” intelligence purpose remains. This reinterpretation of FISA as granting authority both to surveillance and prosecution was a first and momentous step in undermining the divide between nationals and foreigners.

The so-called “wall” between intelligence and law enforcement actually ran parallel to the separation of national citizens from alien residents and protected the former, while facilitating the targeting of the latter. This is strictly in line with high policing, as it was originally exercised. More significantly, perhaps, the breaking down of the barriers between political surveillance and law enforcement weakens the distinction between natives and strangers. It thus aggravates the situation for both. The roundups of foreign suspects residing in the US and preventively detained *incommunicado* is an ominous sign that aliens may become relatively free game in national territories. As for the nationals, there is a risk of their becoming strangers in their own country, if the coordination between law enforcement and intelligence agencies becomes an ordination to a high policing ministry. There is now a movement among US Republicans to abolish the five years sunset clause of the most intrusive dispositions of the USA Patriot Act and make them permanent (Lichtblau, 2003a).

The questions that were put to the secretary of the newly created Department of Homeland Security when he testified in March 2003 before the Senate Appropriations Committee show that the Bush administration is making headway in this direction. Mr Ridge was asked the following question by Senator Arlen Specter (R-PA):

> My next question is what steps can you take when the FBI uses the wrong standard for probable cause under the Foreign Intelligence Surveillance Act? A couple of weeks ago, Director Mueller was here, and we explored that they were using the wrong standard, *more probable than not*, as opposed to *suspicion under the totality of the circumstances,* and they weren't getting the warrants they should have been getting. With you being responsible for homeland security, what can you do to see that the FBI uses the right standard (US Senate Appropriations Committee, 2003: 8, our emphasis).

Secretary Ridge evaded the question, avoiding having to take sides between the Director of the FBI and the influential senator. He referred to the "respectful disagreement" between Director Mueller and Senator Specter and dropped the matter. Senator Specter interjected ominously that his disagreement with Director Mueller was "not respectful". The crucial point about this questioning is that it is wholly directed towards US *internal* security. Not only is the person being questioned the Director of Homeland security, but the whole interrogation relates to the FBI, which is *not* an organization that is mainly targeting foreigners (although it does). The typical high policing conflation of surveillance and law enforcement can not only result in smudging the distinction between citizens of a country and foreigners, but it could trigger a regression to the times when internal dissidence ("subversion") was confused with violent action against the State. Unless it is rigorously monitored, should "suspicion under the totality of circumstances" become a legal standard it may lead us back to the abuses of the past.

The use of informants

In police parlance, there are two kinds of "sources," that is, human sources (undercover police and various kinds of informers) and technical sources (wiretaps, CCTV and all kinds of electronic surveillance devices). The two examples that I discussed – the enlarged terms of reference of the CSE and TIA – point to a substitution of technical sources for human sources in high policing. Although this needs qualification, it is largely true and motivated by the present circumstances.

First, the time is past when one's enemy resembled oneself (Italian Red Brigades in Italy, German Red Army Faction in Germany and IRA in Ulster). Today the most dangerous organisations targeted by high policing agencies no longer originate from the countries they attack (or in which they may reside for periods of time) and they operate on a transnational basis (Buzzetti, 2003b). Consequently, they have a very different ethno-racial make-up than the personnel of these agencies, from whom they differ by the language, religion, mores and physical traits. This affords them no small degree of protection against infiltration. Furthermore, these organizations are very violent and for further protection against infiltration they ask a price for joining them – the commission of a heinous crime, generally murder – that they know no undercover agent and even no informant under the control of a handling officer will be allowed to pay. Contrary to police fiction and journalistic delusions, no undercover police or agents that they control are allowed to commit murder or to put lives in danger in order to be accepted into a criminal organization or to maintain their cover therein, in (democratic) countries that respect the rule of law.

There are several ways out of this predicament. The first one is to recruit as informants persons who are already members of these organizations and who have previously paid on their own their ticket of entry, moving thus from a strategy of infiltration to a strategy "exfiltration" (offering various rewards to an insider for information and for his testimony in court). Generally speaking, the police cannot ignore for long the crimes of these informants when they have been committed on the home territory and informants eventually end up in a witness protection program, testifying against their former accomplices in return for a reduced sentence for themselves. Not only, then, is their time as secret informants limited, but their trustworthiness is doubtful and is increasingly being questioned by the courts, as they tend to bring justice in disrepute. A second solution is to rely on informants controlled by a friendly foreign service that doesn't mind running murderers as informants. The problem with this answer is that it doubles the risk of manipulation for the service attempting to run an informant (who will never be met) through a third party of unscrupulous colleagues. A last resort is to recruit one's own moles abroad, as the Soviet Union did with outstanding success in the UK and, more recently, in the US, with Aldrich Ames. However, the possibility that such moles may be double-agents is always present, as the FBI learned in the Katrina Leung case (Lichtblau, 2003b). In organizations motivated by religion, which now appear as the most lethal, this strategy seems to come up against a wall (although we may learn differently in time). Two years ago, 25 million USD was offered for information leading to the neutralization of Ousama Bin Laden, with no success at the present time (of course Bin Laden may now be dead, which would explain for the dearth of information).

In conclusion, although it is repeatedly claimed that infiltration is the most efficient high policing tactic (Shelby, 2002: 76-79), and although there have been clamours for a return to the use of human sources, many problems will have to be solved to make it viable and efficient in a transnational context characterized by its sectarianism and ruthlessness. For what we know about the history of murderous regimes, they are not easy to infiltrate. The same would apply to murderous organizations. Nevertheless, governments have far from given up on infiltration and are taking measures to solve some of the problems that we have just discussed. Canada, in new legislation passed against organized crime in the beginning of 2003 (Bill C-24), has granted permission to undercover police *and their agents* to commit serious crimes in order to infiltrate criminal organizations and preserve their cover. The law does not list permitted and forbidden crimes in a legal "schedule" (list), since that would defeat its purpose. Of course crimes such as murder, aggravated assault and other grievous violent acts are not covered by this provision, but police may be authorized to commit simple assault (an extensible offence) and deal in drugs in the context of sting and counter-sting operations. These authorizations confirm the notion that high policing cannot be law abiding in all respects and that it cancels out to a significant extent the notion of police deviance.

This neutralization of police deviance is even stronger in technological high policing. This could be illustrated in several ways. As previously stressed, the CSE is prohibited from intercepting the private communications of Canadians. Yet since it scoops up all electronic emanations flying through the atmosphere, it is bound to mostly intercept Canadian communications. There is, we are told, software that is supposed to filter out such communications. But, if it were at times to fail, who (what) could be made accountable? A second example: in Canada and the US one needs a judicial warrant to intercept telephone communications transmitted through land lines, which offer a reasonable presumption of privacy (hence the need for a warrant to intrude upon this privacy). However, when land lines are overloaded, a part of telephone communications is diverted for transmission purposes to telephone towers that transmit them without any wires. Does one still need a warrant to intercept a private communication that is suddenly switched on to a wireless telephone tower? We have no idea. The basic fact is that legislation is always lagging far behind the development of technology. Techno high policing is thus to a large extent outside the reach of any law and the notion of its being deviant is completely short-circuited.

Finally, techno high policing is as potent for generating surveillance paranoia as was the notion of one being surrounded by police informants. The notion that one is under surveillance at a distance generates a feeling of helplessness that is even more chilling than the fear of personal betrayal. One can at least try to uncover a snitch and remove him or her from one's environment. However, trying to get rid of surveillance technology is as self-defeating as attempting to do away with the environment itself.

HIGHER POLICING?

We could conclude that the features of high policing still apply to surveillance as it is now exercised, but with some qualifications. The most significant of these qualifications concerns the now dominant role of technology, which could not be taken into account for historical reasons by the architects of high policing. However, the basic trait of high policing – its relative intractability to the rule of law or, it may be suggested, its a-legality – is enhanced by the dependence upon technology and, more generally speaking, by the present evolution of political surveillance.

However justified, this conclusion is not on all points satisfactory. First of all, high policing is, as we have seen, essentially dependent upon the collection, analysis and dissemination of intelligence. So fundamental is this link that high policing should be described as intelligence-leading rather than intelligence-led policing. In theory, it fills the blanks, moving from one piece of the puzzle to the total picture. In this respect, we have to take stock of the criticism of the capacity of law enforcement organizations and of their personnel to perform this function. Hence we should make a clear distinction between high policing as an ideal type, in the sense of Weber, and high policing as a very incomplete incarnation of this paradigm.

Second, whether invented in France at the end of the seventeenth century as high policing or reinvented in England at the beginning of the nineteenth as low policing, policing always stood as an *alternative to the military*. It is premature to say that this is no more the case. Nevertheless it must be recognized that the militarization of policing, in its diverse aspects, in now a real issue. This issue has taken a particular urgency because of the emergence of mass terrorism, which fits, in their literal sense, neither the legal category of crime nor the political category of war as an aggression perpetrated by an enemy State – although both concepts are metaphorically abused in referring to terrorism. For instance, the US administration has taken to refer to both the police and the military as "war fighters", this metaphor being clearly tipped in favour of the military. Note that both of the agencies that we have described – the CSE and the IAO – answer to departments of defence (at their inception, at any rate).

These developments are significant enough to warrant a new characterization of political surveillance, which does not so much contradict the high policing paradigm as it completes it.

Deductive and inductive surveillance

One of the most important differences between technological surveillance (SIGINT) and surveillance through informants (HUMINT) is that the former is exercised from a distance, whereas the latter implies closeness (infiltration is a tactic that relies on proximity to the target). This ambivalence, between the tactics of proximity that are the defining feature of community policing and the watch from a distance that is a growing trend of surveillance, is characteristic of late modernity policing.

Watching individuals from a close position is an *inductive process* that moves from the particular subject(s) under observation to his or her inclusion into a category of like individuals or to a general conclusion (these persons are enemies of the State and so forth). An initiative like TIA, which relies on the computerized monitoring of a great mass of transactions, is innovative in relation to the traditional inductive conception of surveillance. As we saw, the main component of TIA relied on the extraction of (hypothetically) predictive patterns from a very large sample of terrorist acts (if possible the sample would include all known terrorist acts). These patterns are general, consisting of prototypical sequences of events revealing a hostile intention. Although they are not science, they perform a role that is nevertheless similar to scientific generalisations. Transactions are monitored by computer, without any particular attention being at first given to the individual(s) or groups of individuals engaged in them: the computer is simply attempting to apply general predictive patterns to transactions initially divorced from whoever is performing them (de-nominalized, as we said). However, if a transaction fits a predictive pattern, an alert is given and the system moves into its identification mode, which then directs field officers to intervene. The whole process can be formalized as a tentative syllogism:

Universal premise:	All who engage in pattern A are dangerous
Particular statement:	At least one X is engaging into the performance of this pattern
Alerting Inference:	At least one X (this or these particular X) is dangerous
Identification mode:	Who is X?
Effective identification:	X=A (a)……. A (n)
Normative premise:	All dangerous persons must be stopped
Pragmatic conclusion:	A (a)….A (n) is (are) wanted/arrested for questioning

Deductive surveillance is not limited to political surveillance. It is part of a growing trend in policing, alongside the generalization of profiling. Profiling poses a dilemma where both alternatives are problematic. If the profile is too general, it generates an intolerable amount of false positives; if it is sufficiently precise to exclude false positives, it will also miss a number of true positives and the probability that it is spurious will increase.

Deductive surveillance also is closely in line with one feature of high policing, that is, the accumulation of powers that should remain distinct, as pseudo-scientific laws, predictive patterns and profile supersede legislation and provide norms for pre-emptive repression.

Militarization and privatization

The feature of war that is most obscenely displayed nowadays is that techno proficient countries no longer rely on military personnel in combat. The firepower of Western countries (most notably, the US) is so overwhelming for their enemy that the majority of Western casualties in a war against a non Western power are caused by "friendly fire", as Canadians learned in Afghanistan and as UK troops are now learning in Iraq. It is more hazardous to wage war with the US than against its enemies.

As President Eisenhower aptly said, the military are bound to the industrial complex, which develops its technology. Researchers have also emphasized the strong links between the military, technology and private industry (Haggerty and Ericson, 2001; Kraska, 2002; Leman-Langlois, 2003). To the extent that policing may be under the sway of the military, it is also dependent upon private enterprise. In this respect it is worthy to note that Dr. Charles E. McQueary, a former executive of General Dynamics and Bell Laboratories, is the newly confirmed undersecretary for Science and technology in the Department of Homeland Security. Since the creation of this department, the Homeland Security Research Corporation was established in San José, Calif.; so was the Homeland Security Industries Association, a trade group that has signed more than 100 companies as members since it was incorporated in July 2003.

As we previously argued, the purchase of technology in not governed by what is adequate for the task at hand, as much as it is by what is available on the market. In this respect, the big armaments firm, Raytheon, has announced Project Yankee: "a company wide effort to determine how its military expertise and products might be converted into counter-terrorism" (Shenon, 2003). Our conviction is that change is not brought upon by human policy as much as imposed by the development of technology (let us think about the police cruiser or the personal computer). It is thus to be foreseen that the impact of technology originally conceived for the military will strongly affect domestic policing, for good, bad or worse.

Enemies and law breakers

As always, changes in the stuff of policing will be reflected in our concepts of policing. Up until now, a clear distinction has been made between internal and external security. Internal security meant protection against criminal aggression against one's person and one's property, such aggression being motivated by hatred, lust or greed, but rarely by politics. It was first incumbent upon the public police and, in an increasing way, upon private security to provide such protection. External security referred to protection against aggression by another country, the army being the main instrument of this protection. It now seems that all of these distinctions can be questioned in various ways. The definition of war as violence taking place between different countries is not rich enough to accommodate asymmetric conflicts, where one state is the target of an aggression that is politically and/or religiously motivated, by an international organization based in several countries but belonging to none. The September 2001 attacks are the most dramatic example of asymmetric conflicts. Asymmetric conflicts are hybrids that are test cases for the traditional categories in which it is difficult to fit them in. Due to their complete disregard for the rules governing hostile relationships between states (e.g. ultimatums, declarations of war and so forth), they can be construed as crime and they effectively are. Because of the mass destruction that they bring, they can also be considered as acts of war and they also effectively are. Being both crimes and warlike aggressions, events like 9-11 fall at the same time within the province of internal and external security; as such they are also simultaneously under the purview of the police and the military. The very name of the US Homeland Security Department shows that it is an obsolete umbrella that tries to shade agencies reaching far beyond the US homeland, as even the most cursory examination of its make-up reveal.

I have belaboured the 9-11 example because of its vividness in our minds. However, as de Lint and Virta (2003) have argued, politics are permeating a great deal of crime and of policing. Indeed, it could be claimed that all organized crime, when it reaches beyond gangs that quickly dissolve, has political overtones (Brodeur, 2000). The upshot of these remarks is that political surveillance is now a misnomer and that we should just talk plainly of surveillance, as Foucault did.

Surveillance-fiction

Allan Greenspan, the chairman of the US Federal Reserve, coined some years ago the expression “irrational exuberance” to stigmatize the speculation fever that produced the stock market “bubble” that erupted shortly after his comment. This phrase also applies to the present context. Technology, it is brashly claimed, will remedy all the past failures of intelligence. This effervescent surveillance bubble may well burst, like the previous one, and make a score of victims (not to be found among the surveillants but among their “collateral” targets). The problem is that under national security secrecy legislation, we will not know about it and that many people will be hurt without any external means to control the damage.

The now infamous FutureMap project (Futures Markets Applied to Prediction), which precipitated the end of the IAO, is a great illustration of this surveillance bubble. This program was developed to predict international events based on how an “events futures” market would behave. There cannot be a more self-defeating claim as this one. Predicting how stocks are going to evolve has always been a losing game, as nearly all heads of mutual funds that haven’t been yet fired can testify to. One would hope that such dud technology will not be used to plot the next moves of Al Quaeda.

Yet it probably will, in one guise or another, no matter how facetious. There is now such craving for intelligence that this is an irrational sellers’ market. One consequence of this predicament is the maximization of the possibilities of making mistakes. There is something that no software can do by itself: it is inputting the data. The current illusion is that police, who are said to be poor analysts, will prove better as data collectors. They will not, if they are not trained to be better. In the present context marked by a high level of immigration, just spelling a name consistently is a considerable challenge that is not met. The more encompassing and sophisticated our data collecting and processing devices are, and the higher the possibilities for making errors. Just recently, the US Justice Department has identified some 3 000 criminal cases that could have been affected by flawed procedures and skewed testimony by FBI laboratory technicians up until 1997 (Associated press, 2003). The bigger the science and the bigger is the shadow of mishaps that it projects. Scientists have developed a large safety net against such miscarriages, but the police have not yet.

In his original 1983 paper Brodeur claimed that the net cast by high policing mainly caught distraught fishes that swam headlong unto them. Shortly following 9-11, the venerable French composer and orchestra director Pierre Boulez, who once headed the New York Philharmonic, was detained for several hours by the Swiss under suspicion of being a terrorist. It happened that under the pandemonium prevailing in France in May 1968, Pierre Boulez, then a young artist, proclaimed that opera houses should be "burned down" (setting fire to something was then trendy). This was not forgotten by the police and Boulez was branded as a terrorist in some buried file, which resurfaced in some small border crossing booth, after September 2001. Being a celebrity, Monsieur Boulez was quickly released with the profuse apologies of the Swiss authorities that had invited him to their music festival. An unknown Arab student previously given to despondent rhetoric, as many students were at that time, might not have fared as well.

What we should be worried about is not the Big Brother, but the Big Bungler. Not only is he well, alive and uncontrolled, but he may be thriving in the years to come, particularly now that Saddam Hussein has been made to shed his public skin as the Head of the State of Iraq and to join forces with invisible terrorists. Big Bungler is in no way a fumbling Mr. Bean substitute for Big Brother, which we need not worry of. On the contrary, Big Bungler is Big Brother driven mad by too much power and too much Speed. It offers little protection against the Meanies and might hurt all the wrong people.

Paris/Montreal
June 28, 2003
Jpb/S l-l

REFERENCES

Associated Press (2003), "Errors at F.B.I. May Be Issue in 3 000 Cases", *The New York Times,* 17.03.03.

Bamford, James (1982), *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, New York, Penguin Books.

Brodeur, Jean-Paul (2003), "The Globalization of Security and Intelligence Agencies: a Report on the Canadian Intelligence Community" in Brodeur, Jean-Paul, Peter Gill and Dennis Töllborg (2003), *Democracy, Law and Security. Internal Services in Contemporary Europe*, Aldershot, Ashgate, 210-261.

Brodeur, Jean-Paul (2000), "Cops and spooks", *Police Practice and Research*, Vol. 1, No. 3, p. 299-321

Brodeur, Jean-Paul (1992), "Undercover policing in Canada: Wanting what is wrong", *Crime, Law and Social Change*, No. 18, p. 105-136

Brodeur, Jean-Paul (1983), « High Policing and Low Policing: Remarks About the policing of political Activities", *Social Problems*, Vol. 30, No. 5, 507-520.

Buzzetti, Hélène (2003a), "Surveillance internationale. Ottawa rend plus acceptable sa banque de données sur les voyageurs", *Le Devoir*, 10.04.03.

Buzzetti, Hélène (2003b), "Rapport de la Vérificatrice Générale du Canada. Le Canada a perdu la trace de 36 000 immigrants illégaux », *Le Devoir*, 9.04.03.

Canada, (1981), *Freedom and Security under the Law: second report, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (The McDonald Report)*, Ottawa, Minister of Supply and Services.

Communications Security Establishment Commissioner (1997), *Annual Report, 1996-97*. Ottawa: Minister of Public Works and Government Services Canada.

DARPA (2003a), *Fiscal Year (FY) 2004/FY 2005 Biennial Budget Estimates*, February 2003.

DARPA (2003b): Report to Congress Regarding the Terrorism Information Awareness Program. In response to Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division M, § 111(b). http://www.darpa.mil/body/tia/TIA%20DI.pdf .

De Lint, Wilhelm and Sirpa Virta (2003), *Security from politics: Low and High Policing Revisited*, paper presented at the "In search of Security Conference", Montreal, Law Commission of Canada, February 2003.

Firestone, David (2003), "Senate Rolls a Pork Barrel into War Bill", *The New York Times*, April 9, 2003.

France (2003), *Rapport à l'Assemblée nationale, renseignement; Rapporteur spécial: M. Bernard CARAYON*, Document #256.

http://www.assemblee-nat.fr/12/budget/plf2003/b0256-36.asp

Frost, Michael and Michel Gratton (1994), *Spyworld: Inside the Canadian and American Intelligence Establishments*, Toronto, Doubleday.

Haggerty, Kevin D. and Richard E. Ericson (2001), "The Military Technostructures of Policing", in Peter B. Kraska (ed.), *Militarizing the American Criminal Justice System*, Boston, Northeastern University Press, 43-64.

Hakim, Danny and Nick Madigan (2003), « Immigrants Questioned by F.B.I. », *The New York Times*, March 22, 2003.

International Herald Tribune (2003), « New Airport Profiling », Editorial (unsigned), March 11, 2003, p. 6 (the IHT is published by *The New York Times*).

Kraska, Peter B. (2002), *Militarizing the American Criminal Justice System*, Boston, Northeastern University Press.

Laudon, Kenneth C. (1986), *Dossier Society: Value Choices in the design of National Information Systems*, New York, Columbia University Press.

Leman-Langlois, Stéphane (2003), "The Myopic Panopticon: the Social Consequences of Policing Through the Lens," *Policing and Society*, 13 (1), 43-58.

Lichtblau, Eric (2003a), "Republicans Want Terror Law Made Permanent", *The New York Times*, April 9, 2003.

Lichtblau, Eric (2003b), "F.B.I. Was Told Years Ago of Possible Double Agent", *The New York Times*, April 12, 2003.

Plenel, Edwy (1997), *Les mots volés*, Paris, Stock.

Privacy Commissioner of Canada (2003), *Annual Report to Parliament, 2001-2002*, Ottawa, Privacy commissioner of Canada (also available at http://www.privcom.gc.ca).

Québec (1981), *Rapport de la Commission d'enquête sur des opérations policières en territoire québécois* (rapport Keable), Québec: ministère des Communications.

Risen, James (2003), « C.I.A. Aides Feel Pressure in Preparing Iraqi Reports », *The New York Times*, March 23, 2003.

Sallot, Jeff (1984), « Secret agency keeps data on individual "security risks" », *The Globe and Mail*, 21.11.84, 1.

Shelby, Richard C. (2002), *September 11 and the Imperative of Reform in the U.S. Intelligence Community. Additional views of Senator Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence*, United States Senate Select Committee on Intelligence, Washington D.C.: US Government Printing Office. (This report is also available on the Internet at http://intelligence.senate.gov/pubs107.htm)

Shenon, Philip (2003), "Domestic Security: The Line Starts Here", *The New York Times*, March 6, 2003.

Skolnick, Jerome (1966), *Justice Without Trial*: *Law Enforcement in a Democratic Society*, New York: John Wiley.

United States Senate, Appropriations Committee (2003), *Full text of Testimony Before the Senate Appropriations Committee*,

http://www.nytimes.com/2003/03/27/international/worldspecial/28FTEX-RUMS.htlm.

United States, Congress (2002), *Joint Inquiry conducted by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Findings and Recommendations*, Washington D.C.: US Government Printing Office. (This report is also available on the Internet at http://intelligence.senate.gov/pubs107.htm)

United States, Congress, House, Select Committee on Intelligence (1977), *CIA : The Pike Report,* Nottingham, Spokesman Books for the Bertrand Russell Peace Foundation

United States, Congress, Senate, Select Committee to Study Governmental Operations With Respect to Intelligence Activities, 94th Congress, 2nd Session (1976), *Intelligence Activities and the Rights of Americans* (The Church Report), Washington (D.C.), US Government Printing Office.

Websites

1. EPIC (Electronic Privacy Information Center):
http://www.epic.org/privacy/profiling/tia
2. FERET and Face Recognition Vendor Test: http://www.frvt.org
3. Government exec.com:
http://www.govexec.com/dailyfed/1102/112002ti.htm
4. IAO: http://www.darpa.mil/iao/index.htm
5. New Tools for Domestic Spying, and Qualms (*Cryptome*)
http://cryptome.org/tia-balk.htm
6. New York Times:
http://www.nytimes.com/2002/11/09/politics/09COMP.html

7. Total Information Awareness Program (TIA) System Description Document (SDD) (Official Document, 150 p.).
http://www.epic.org/privacy/profiling/tia/tiasystemdescription.pdf

8. Washington Post:http://www.washingtonpost.com/ac2/wp-dyn/A40942-2002Nov11