

Privacy Games
The Vancouver Olympics, Privacy and Surveillance

**A Report to the Office of the
Privacy Commissioner of
Canada Under the
Contributions Program**

March 2009

Authors

Philip J. Boyle
Department of Sociology
University of Alberta

Kevin D. Haggerty
Department of Sociology
University of Alberta

c/o
Department of Sociology
University of Alberta
Edmonton, Alberta, Canada
T6G 2H4

Executive Summary

The Olympics now amount to a machine for change, helping to initiate transformation in the host city and country that take place at different levels and culminate in legacies that persist long after the closing ceremonies. This includes legacies that are manifest at the corporate, urban and political levels.

Olympic officials typically accentuate the positive legacies that the Games can produce in terms of new stadia, infrastructure projects, and even national pride and collective memory. There are, however, some less discussed Olympic legacies pertaining to security and surveillance that deserve attention. Since the 1972 Munich Games, when Palestinian militants murdered 11 Israeli athletes, event organizers have been anxious about security. Such fears were borne out again when Eric Rudolph detonated a bomb at the Centennial Olympic Park during the 1996 Atlanta Olympics, killing one person and injuring over 100 others. The recent spate of terrorist attacks in New York, Washington, London and Madrid have put security on the agenda like never before, altering the face of the Games while also producing a host of wider technological and attitudinal changes. More

recently, the targeting of the Sri Lankan national cricket team in Pakistan provides yet another reminder that sport is not immune from political violence.

The September 11th terrorist attacks helped radically expand the corporate market in security products and services to such an extent that we can now speak of a global 'security industrial complex.' While Olympic security only accounts for a fraction of the total amount spent on security internationally, the security price tag for these events can still be impressive. Close to \$1 billion (CAN) is now budgeted for security for the 2010 Games, well beyond the initial estimate of \$175 million (CAN). Security costs cover many things, but in the current context one cannot separate security from surveillance. A raft of security measures aim to make people, places and processes visible in new ways using diverse tactics and technologies. Some of the notable surveillance-related technologies and practices that have been deployed at recent Games include biometric identification cards, toxic material scanners and detectors, computerized background checks, CCTV cameras, magnetometers, satellite monitoring, cellular telephone monitoring (both legal and

illegal), overhead communications/ monitoring blimps, traveller profiling and the increased integration of artificial intelligence into a host of private and public sector databases. In addition to the bewildering variety of surveillance measures employed to secure the Games, the integration of various surveillance technologies is perhaps one of the most remarkable and, from a privacy perspective, disconcerting facets of Olympic security efforts.

Security considerations make the Olympics important moments in the development and dispersal of surveillance. Public officials occasionally use the pretext of the Olympics to introduce forms of surveillance that the public might oppose in any other context, capitalizing on the fact that in anticipation of the Games citizens tend to be more tolerant of intrusive security measures. As the Games are bounded in space and time, security planners also treat them as an opportunity to conduct real-world tests of new informational and technological systems. The Olympics have consequently become a crucible for experiments in monitoring. After the Games, however, these systems may not disappear but stay, delivered and justified as public safety and/or counter-terrorism enhancements that

will serve the host city and country for years to come.

Such developments are important because of the wider surveillance legacies of the Games. Executives, drawn by the prospect of a financial windfall, are developing innovative, intensified and integrated monitoring technologies specifically for the unique risks posed to the Olympic Games. In the process, the surveillance infrastructure established for the Olympics expands and each new iteration becomes the standard to build upon for future Games. Moreover, security firms capitalize on the prestige of their Olympic involvement to promote their technologies and systems as security solutions for other major events and more prosaic security situations. Designed for the unique risks of an exceptional global sporting event and driven by the search for new markets and profits, the technologies, expertise and contacts characteristic of Olympic security therefore risk dispersing into more mundane contexts, simultaneously routinizing and intensifying security.

Beyond the role of the Olympics in creating and extending new surveillance measures, the Games can also shape public attitudes in ways that are both vital to understand but difficult

to demarcate. The tremendous global media attention dedicated to the Games now involves a steady drip-feed of stories about security preparations. Reporters photograph rooftop snipers, map security zones, and provide wide-eyed accounts of the technological abilities of new screening technologies. Such stories cumulatively amount to a form of public instruction in the 'new realities' of security. Citizens are familiarized with the new routines of high security, a process that helps normalize practices that might otherwise be seen as intrusive. The proliferating security routines characteristic of the Olympics therefore fosters a security-infused pedagogy of acceptable compartment, dress and documentation, as small lessons in security are inflated and played out before a global audience. This reinforces the sense to which it becomes self-evident that such measures are required, that they do not unduly infringe upon personal liberties, that certain dangers are pervasive – and more pressing than other risks – and that the existing constellation of security interests is inevitable.

Such legacies have emerged from many previous Olympics in recent decades. However, in the post-9/11 period, these legacies are no longer accidental, unintended or partial outcomes. They, like transportation improvements and property development, are entirely planned deliverables, just another beneficial outcome to be 'leveraged' from an opportune moment. As these legacies continue to reach beyond the time and space of the event, the Games themselves provide a glimpse of a possible militarized, surveilled urban future.

The Vancouver 2010 Olympics will undoubtedly provide unprecedented opportunities for a global audience to witness memorable athletic performances. We also need to contemplate whether one unanticipated consequence of the Games is that we, as Canadian citizens, might not also find also ourselves visible in ways for which we had not bargained, a visibility that inevitably involves diminished personal privacy.

Introduction

Drawn by national pride and the prospect of witnessing world-class athletic performances, an enthusiastic global audience has made the Olympic Games some of the most observed events in history. The sheer scope of this viewership has also meant that for a long time now the Olympics have been far more than a sporting event. Massive international audiences, combined with the promotional efforts of Olympics organizers, have made the Games one of the world's premiere corporate sponsorship venues and advertising platforms. For organizers a large part of the appeal of the Games is that they provide an opportunity to fashion and promote an attractive image of the host city and country to these same audiences, something that is important for national pride but also for international trade and tourism (Hiller 2006). Looking forward to the 2010 Olympics and Paralympic Games¹, the City

¹ For clarity sake we use the expression 'the Olympics' or 'the Games' in this document to include both the Olympics as well as the Paralympic Games that follow the Olympics. We are aware that these are separate events that present different types of security and safety concerns.

of Vancouver presented these events as providing:

“an opportunity for the City of Vancouver to foster civic pride and a greater sense of community in our residents, to create positive experiences and fond memories for our visitors, and to captivate the media through a festive environment, positive images and broad exposure to one of the most liveable cities in the world” (City of Vancouver 2006a: 4).

For organizers, however, the extensive publicity of the Games is a mixed blessing. It is now routine for protesters to use the Games' global media profile as an opportunity to advance various social causes. While some might see this as regrettable, such non-violent protest is a legitimate and ultimately laudable attribute of living in a free society.

More disturbing is the prospect that terrorists² will target the

² The term 'terrorist' is famously difficult to define, as one group's terrorists are another's freedom fighters or guerrilla soldiers. For our purposes here we simply treat terrorist *extremely* broadly as those individuals who would use violence to disrupt the Olympics to further a social or political cause. We leave it to others to determine whether such individuals fit

Games. While terrorism is often equated with the use of random violence, terrorists need not be violent. For example, using remote computers to hack into and bring down a city's electric grid could qualify as a terrorist act, although it would not be straightforwardly violent. Terrorism is, at its heart, an act of communication. Terrorists use violence and disruption to communicate a series of unambiguous messages; that they can access ostensibly secure locations, that people are not safe, that the state cannot protect its citizens. They also use the public and media attention that is drawn to their actions as a forum to communicate more specific messages that pertain to individual causes. Terrorists can therefore also be attracted to the Olympics because it provides them the prospect of using violence and disruption to capitalize on the assembled global media to communicate to a massive international audience (Tulloch 2000).

The modern history of violence at the Games is inescapably linked with the 1972 Munich Olympics when Palestinian militants killed eleven Israeli athletes. This connection was reinforced when a pipe bomb was detonated in Atlanta's

within accepted popular understandings or legal definitions of what constitutes a 'real' terrorist.

Centennial Olympic Park during the 1992 Games, killing two people and injuring 111 (Cottrell 2003). And while the terrorist attacks on the United States on September 11th, 2001 (hereafter '9/11') did not occur in the context of the Olympics, those attacks were so unprecedented in terms of their scale, lethality and boldness that security officials have had to re-think the security dynamics of all large, media-saturated events where substantial crowds gather (see Wong 2001 for example). The 2004 train bombings in Madrid and the 2005 attacks on London's transportation system have only accentuated the fact that large open systems are difficult to secure and therefore make attractive terrorist targets. More recently, the March 3rd 2009 targeting of the Sri Lankan national cricket team by armed militants in Pakistan provide yet another reminder that high-profile sporting events can present an attractive platform for those wishing to convey their message through violence.

Peter Ryan, leading security consultant for the International Olympic Committee (IOC), recently expressed the view that it is 'only a matter of time before terrorists target a major North American sports venue' (Houston Chronicle 2007). At least one journalist in Vancouver has speculated on the likelihood

of a major terrorist attack on the 2010 Games (Smith 2005). Anxious segments of the public share this sentiment. Even in a context where no specific terrorist threats targeting the Vancouver Winter Games have been publicly identified, fully one quarter of the residents of British Columbia asked in a national poll conducted one year prior to the Games believed a terrorist attack would occur before or during the Winter Olympics (Curry & Friesen 2009).

Given that the Olympics are attractive terrorist targets, officials must work to thwart individuals who would disrupt the Games while also establishing contingency plans to deal with the eventuality of a successful attack. At the same time, planners are always dealing, to some extent, with an unknown. Even supported by large budgets, dedicated staff and the best available intelligence, it can be difficult, if not impossible, for officials to determine the real likelihood of a terrorist attack.

In the post-9/11 environment the Olympics have consequently become full-scale exercises in national security that necessitate extensive and increasingly expensive security preparations. A diverse array of tactics and technologies are incorporated

into securing the Games. Prominent amongst these measures is the use of surveillance.

Surveillance should not be narrowly construed as simply referring to spies or CCTV cameras. Instead, surveillance involves collecting and analyzing information about populations in order to direct their behavior. This includes simply monitoring the prevalence and dynamics of assorted risks, but also more directed attempts to use surveillance to try and solve particular problems. Such monitoring now comes in an astonishing array of forms and configurations, and can incorporate such things as satellite imaging, assorted official documents and credentials, wiretapping, radio frequency identification chips (RFID), data mining, X-rays, DNA, assorted forms of biometrics (iris scans, fingerprinting, facial scans, gait analysis), and many other things.

As we detail below, security efforts for the Olympics now draw upon and integrate a plethora of surveillance technologies. The Games also represent particularly important moments in expanding, intensifying and normalizing surveillance practices.

While the general public has become attuned to some of the

security threats posed by terrorism, other factors also drive the use of surveillance at the Olympics. Safety, in particular, is also a prominent concern. Here 'safety' is understood to consist of assorted risks of untoward events that are serious and disruptive, but are not the result of the actions of militants or terrorists.

Some of the potential safety concerns that might hypothetically arise during the 2010 Games include a flood of the Lower Mainland, an earthquake, major fire, excessive snowfall, or the (spontaneous) collapse of the Lions Gate Bridge. Indeed, the number of potential safety concerns that officials must contemplate is astounding. Many of these safety risks are managed as a matter of course in the routine operation of the public safety infrastructure. The Olympics, however, brings with it new safety issues and intensifies existing worries. The sheer number of people who visit the Games places added pressures on many components of the host city's infrastructure, particularly the transportation system. The fact that large segments of the people in attendance will be new to the city or country, and might not speak English or French as their first language, can also compound the downstream

difficulties should something go wrong.

While it might be tempting to consider these safety issues as a less pressing concern than that of security threats, in the past thirty years comparatively few people have died from intentional acts at large sporting events. Many more individuals have died as a consequence of dangers that would be characterized as 'safety' issues, including collapsing bleachers, riots, stadium fires and food poisoning (Stevens 2007).

Safety issues are a serious concern to organizers because of the dangers they pose to the health of citizen and visitors, but also because they can detract from the project of impression management that is so central to an Olympics' success. Here, the specter of the Atlanta Summer Games looms large, as many people remember those games not because of the athletic performances, but because of the Centennial Park bombing and Atlanta's well-publicized traffic chaos. Indeed, traffic is a particular concern for the organizers of the Vancouver Games given the prospect of disastrous traffic interruptions if the Sea to Sky highway were to be blocked, as it is the main route connecting the city of Vancouver with the town of Whistler where the majority of the sporting

events will be held. Such concerns turned acute in August of 2008 when a landslide of an estimated 16,000 cubic metres of rubble closed the highway for several days.

Olympics organizers must also be conscious of routine forms of criminal behaviour. This includes the escalation of predatory crimes which can occur as criminals are also drawn to the illicit opportunities provided by the large Olympic crowds, including robberies, pick pocketing and thefts from cars (Decker, Varano, & Greene 2007).

In Vancouver, many of these crime-related anxieties fixate on the Downtown Eastside (DTES). This neighbourhood consists of approximately 16,000 residents and has the lowest socio-economic status of any urban area in Canada. The median income for people living there is \$14,024. More than 40% of its residents receive some form of income assistance (City of Vancouver 2006b), and the average annual income, minus government subsidies, is only \$6,282 (Matas & Lehmann 2009). It is also home to a disproportionate number of Vancouver's drug addicts and mentally ill. The approximately 6,000 intravenous drug users in the area and the active sex trade have contributed to a serious

problem with Hepatitis C, and the highest per capita HIV infection rate in North America (Health Canada 1995), prompting the City of Vancouver to declare its first-ever medical emergency in 1997. To further compound the area's problems, alcohol abuse is rampant, exacerbated by the disproportionate number of pubs and liquor license seats in the neighborhood (City of Vancouver 1998).

Long viewed as a policing problem, the Downtown Eastside is home to about three percent of the city's population, but statistics for 2002 show that approximately 19% of all recorded serious violent crimes occur here (City of Vancouver 2006b). In that same year, 36% of all recorded drug offences took place in the Downtown Eastside (City of Vancouver 1999). Few businesses remain and entire blocks of storefront property on the main thoroughfare of Hastings Street are boarded up. Pawnshops are the only thriving commercial interest in the area (Matas 2001) while police and drug users alike acknowledge that local corner stores are often fronts for the illegal drug trade (Huey 2007).

For Olympics organizers, all of these problems are compounded by the fact that the DTES also lies immediately adjacent to

Vancouver's central business and retail districts (Lees 1998; City of Vancouver 2001; MacPherson 2001). The prospect that Olympic visitors will inadvertently wander from Gastown's high end tourist shops into the open drug and prostitution market of the DTES presents risks of criminal victimization and also the prospect of public relations disasters. Indeed, almost since the moment it was announced that Vancouver had won the Olympic bid officials have been anxious about how to 'deal with' the DTES in the context of the Games (Armstrong 2003). Any concerns organizers have that media attention to the problems in the DTES might detract from the image they want to convey of Vancouver being 'one of the most livable cities in the world' were certainly not diminished by the *Globe and Mail* running a front page story on February 14th 2009, proclaiming the DTES to be 'Our Nation's Slum.'

The point in briefly drawing attention to some of these security, safety and crime issues—all of which are informed by a Olympics-inspired desire to display the best possible image of the City of Vancouver to a global audience—is to accentuate how the existence of these and other concerns in the context of the Olympics provide an added

stimulus to turn to various manifestations of surveillance to identify, manage and ideally resolve these problems; problems which operate at quite different levels.³

Like investments in transportation infrastructures or major urban development projects, Olympic-related investments in security, safety and surveillance are often delivered and rationalized in terms of their legacy impact. In the domain of public safety, law enforcement, and counter-terrorism these legacies can consist of improved inter-agency working capacities, organizational modifications, specialized skills enhancement, investments in public safety

³ Although it is beyond the scope of this report, it is worth mentioning that fears about cheating at the Olympics, and in global elite sport more generally, have also been responded to through a host of surveillance measures. This now includes measures to test for assorted drugs and masking agents; something that is done at the Games themselves but now also consists of a regime of unannounced out-of-competition testing, which allows 'doping governing authorities to test athletes anywhere and anytime without any prior notice' (Park 2005). Similarly, the global transmission of disease is a problem accentuated by the Olympics and other large-scale gatherings as they bring together large numbers of people from around the world within close physical proximity for extended durations. As such, the epidemiological dimension of mass gatherings is another facet of major events where surveillance practices have increased exponentially (Lombardo *et al.* 2008).

technologies, or legislative /policy changes.

One prominent example of an organizational legacy stemming from the Olympics Games is the German response to the murders at the 1972 Munich Olympics. Soon after this tragedy Germany created *Grenzschutzgruppe 9* ('Border Guard Group 9', or GSG9), that country's elite counter-terrorism and special operations unit (Reeve 2000). This example is notable not for the privacy issues it may or may not raise but for how it serves to underline the point that the Olympic Games (or other major, non-routine events) can sharpen the perception for needed changes.

The creation of the GSG9 was, however, a retrospective action taken in response to a previous failure. In contrast, recent Olympic Games have been proactively positioned as catalysts for long-desired public safety, law enforcement, and counter-terrorism developments. An early example of this took place in 1980 when planners for the Lake Placid Olympics expected to turn the Olympic Village into a minimum security prison after the Games concluded. In a more recent example, Greece took advantage of the 2004 Olympics to parlay its long-standing participation in the US's Anti-Terrorism

Assistance Program to develop its expertise in a series of law enforcement and counter-terrorism specialties such as VIP security, port and maritime security, canine explosives detection, and crisis response. The Greeks also received training assistance from Israel on how to identify and neutralize suicide bombers (Migdalovitz 2004; GAO 2005). Similarly, China created and trained the elite counter-terrorism unit 'Snow Wolf' in advance of the 2008 Beijing Games (Spencer 2008).

More mundane but no less relevant skills development accelerated by the Beijing Games included training for law enforcement officers in how to effectively communicate with western tourists (provided in Canada by BC's Justice Institute) and high-speed vehicle pursuit maneuvers (The National Post 2006; Sinoski 2008). Consistent with this pattern, the Vancouver Police Department (VPD) has announced it is training a counter-terrorism unit that will support Olympic security efforts before and during the 2010 Games and will continue operations afterwards in conjunction with the RCMP's Integrated National Security Enforcement Team (INSET) already in Vancouver. The creation of this unit mirrors the creation of the VPD's crowd control unit that was developed

in time for the 1993 Clinton/ Yeltsin summit and which has subsequently grown from its initial contingent of 40 officers to a complement of approximately 120 officers.

These examples are intended to underline how the contemporary Olympics are often used as occasions or catalysts for the development of public safety, security, and/or law enforcement legacies that connect both to the short-term requirements of the event as well as long-term needs of the host city/country. These legacies have become explicit objectives of organizers, and are not the accidental, partial, or reactive outcomes of hosting the Games.

Proactively leveraging the Olympics for such legacies is stock advice for at least one official with significant Olympic security experience. Speaking at a post-2002 Olympic Games security debriefing conference, Peter Ryan, former Chief of the New South Wales Police Force during the 2000 Sydney Games and current senior security advisor for the IOC, advised that Olympic security efforts can have a 'huge and lasting impact on national security' that should be 'preserved and absorbed and developed further' (Ryan 2002: 24-25). Ryan continued his remarks by advising that the investment in security

infrastructure for the Olympics could be an 'enormous legacy for the country and its national security capability after the Games. This opportunity should not be wasted' (Ryan 2002: 26). Facing criticisms about the escalating security budget for the Vancouver Games, the International Olympic Committee President, Jacques Rogge echoed Ryan's point, indicating that Vancouver's Games would leave a legacy in terms of better security expertise and hardware 'that will serve the country... for decades to come' (Mickleburgh 2009b).

As we outline below, much of this legacy entails an increase in surveillance capacity. Any use of surveillance also involves an inevitable loss of privacy. For our purposes here, we are concerned with how the Olympics can result in a loss of 'social privacy,' which should be distinguished from questions about 'legally protected privacy.' Something is private to the extent that it is free from scrutiny, and where a person maintains effective control over who is allowed to access and use their information. Social privacy is a larger order concept, one that subsumes the smaller realm of legally protected privacy, the latter of which consists of those realms which are preserved by national and international legislation.

To succinctly make the point about the relationship between social and legally protected privacy, the fact that in advance of the Winter Olympics officials plan to photograph Vancouver neighbourhoods using high-resolution satellite-mounted cameras entails a reduction in social privacy. Satellite imaging is a fairly new and intensive way for physically dispersed audiences to view phenomena that were previously more difficult to monitor. Moreover, such images can sometimes allow viewers to make inferences about a person's lifestyle or interests (whether the satellite images reveal a backyard pool, swing set, compost box or beer fridge, for example, obviously implies something about the homeowner). That said, this satellite-produced reduction in social privacy is not an instance of legally protected privacy, as such monitoring has not been deemed to violate established privacy protections.

While security or policing officials often feel constrained by legal privacy rights, the broad social trend of the past quarter century has involved an unambiguous reduction in social privacy. In Canada, this has occurred in a context where the *Canadian Charter of Rights and Freedoms* is understood to provide basic privacy protections, specifically

embedded in Section 7 which protects a person's 'right to life, liberty and security of the person' and also Section 8 which places restrictions on 'unreasonable search and seizure.' Notwithstanding these legal rights, the lives of individuals, as well as assorted places and processes, have been opened up to unprecedented forms of scrutiny by public and private institutions. Privacy advocates therefore spend a great deal of their time evaluating whether an escalating and expanding range of measures that reduce social privacy might amount to infringements of legal privacy (Bennett 2008).

For our purposes here we are not concerned with tracing instances of privacy *infringements*—which can entail both breaches of legally protected privacy rights as well as more subjective assessments that someone's privacy has been violated, irrespective of the legality of such measures. Instead, we are concerned with the larger and first order question of how the Olympics can cumulatively result in immediate and long-term reductions in social privacy. These reductions are important to document as they can serve as early indicators that we may be building a slippery slope that could be difficult to disassemble.

We delineate these indicators, dynamics and drivers of surveillance initiated in the context of the Olympics, and leave it to others to ascertain whether, and under what circumstances, these might constitute legal or personal violations.

Identifying the surveillance and privacy issues of an event like the Olympics in advance of the Games themselves presents a host of difficulties. The most obvious is that officials are understandably reluctant to detail the specifics of their security arrangements. There are legitimate concerns that publicizing security measures can provide an advantage to those who might want to disrupt the Games. Consequently, much of the specific information that one might want to acquire about the operation of various security systems is classified, and officials are generally tight lipped about their preparations. While this is true of the Vancouver Winter Olympics, it is also generally the case with all mega-events; security officials do not talk about their security arrangements in anything but the most sweeping generalizations before the event.

Our findings in this report are therefore drawn from a number of other sources. Most specifically we analyze how security has been managed at

previous mega-events such as the Olympics, World Cup, Super Bowl and the like. While Vancouver will obviously not duplicate these arrangements exactly, security planners for all mega events must face a series of comparable questions about crowd control, and how to secure venues, athletes, electronic systems, and so on. Strategic advice on these issues is now shared among a global network of security officials who speak at international conferences, write in specialized publications, and have developed numerous mega-event security 'best practices.' After each Olympic Games, and many other mega events, security officials also produce after action reports that detail lessons learned. Those and comparable documents provide valuable insights into the realities and challenges of Olympic security.

While this report was researched and written over the past year, it also builds upon the knowledge, documents and interviews that we have amassed over the past several years as part of a larger research project we are conducting on security at mega-events. We did, however, undertake a series of interviews specifically in aid of producing this report. In October 2008 we travelled to Vancouver to speak with and interview ten individuals who have different

types of involvement in Olympic security. This included a discussion with RCMP Assistant Commissioner Bud Mercer, who is heading the Vancouver 2010 Integrated Security Unit (V2010-ISU) responsible for the overall security of the Games, as well as talks with officials involved in safety preparedness, a security official with the Vancouver Olympic and Paralympic Organizing Committee (VANOC), and also private citizens concerned about the security implications of the Games.

It should be noted that in our preliminary discussions with Assistant Commissioner Mercer, he made it quite clear that there is now a global media fascination with Olympic security. Consequently, the V2010-ISU has felt compelled to develop a policy that they do not grant interviews about even non-sensitive security issues because simply responding to all of these requests for information and interviews risks overwhelming the unit. Hence we are particularly grateful that Assistant Commissioner Mercer and other members of the wider Vancouver public safety contingent were willing to speak with us.

In October 2008 we also travelled to London, England, to attend the Rushman's Sports Security Summit. This high

profile security workshop was populated by a host of mega-event security planners, many of whom have experience with Olympic security, including a security official from VANOC. The Rushmans' event allowed us to participate in many workshops on mega event security, accumulate additional documentation and also interview 14 world leaders in event security on the trends, dynamics and tensions in sport mega event security.

From these assorted sources we have been able to ascertain some of the main trends in mega event security. It is important to stress, however, that the existence of previous security patterns does not mean they will be faithfully replicated in Vancouver. These patterns interact with differing legal regimes, pre-existing public safety capabilities, and widely divergent financial resources that will generate unique context-dependent outcomes. Hence, while we can anticipate some of the security attributes for the Vancouver Winter Olympics, Canadian citizens will not learn about the full scope or particulars of this operation until some time after the Games have concluded. That said, commonalities in the wider circumstances shared by host countries and cities suggest that commonalities amongst solutions can also be expected.

Our research has identified several key changes that the Olympics tend to bring about in relation to surveillance and privacy. The remainder of this report sets out those phenomena and explores them in some detail. We commence by discussing organizational issues pertaining to safety and security management at the Olympics. It is important to begin with this topic as any changes implemented in surveillance practice are ultimately accomplished by organizations, and in the case of the Olympics this can involve the need to coordinate among a staggering number of institutions. Moreover, the Olympics serve as a catalyst towards different types of organizational transformation, typically involving new organizational forms, changes to communication structures and lines of authority. We move from that topic to discuss how security for mega-events has become an increasingly large and profitable business. The Olympics are an important moment in this wider security industry both as a site

for lucrative contracts, but also as a global showcase for new security and surveillance initiatives, many of which involve information, visualization and communication technologies. Our third section specifically focuses on detailing some of these new technologies and how they have been used at the Olympics and other mega events.

The Olympics also give rise to a host of mundane policing issues; a topic we explore in three subsections. The first addresses how previous Olympics have often contributed to increased efforts to police the poor and marginal segments of the host city. The second policing issue is much more specific to the Olympics, in that it involves efforts to protect the commercial rights associated with the Games; something that can culminate in citizens being subjected to quite distinctive forms of scrutiny. Finally, the Olympics also bring added pressures of policing protest and dissent, a topic we explore in the final subsection.

Organizational Structure and Integration

Security for the Olympic Games is a massive and complex task. Security officials often describe these efforts as the 'largest peacetime security effort' of their respective host country. One Olympic security official goes further, noting that 'wars have been planned and executed in less time and with less people' (Ryan 2002: 24).

This complexity arises from a number of factors. Protecting large numbers of people spread across entire cities (sometimes more than one city) at dozens of venues creates a host of mundane public safety concerns and gives rise to routine forms of crime. Hundreds of athletes and thousands of media officials and visiting diplomats need to be accredited. Domestic officials of varying ranks and visiting political figures, even heads of state, require special protection. Indeed, even the logistics of housing and supplying the considerable contingent of security personnel is a daunting task, a problem the RCMP has recently run into (Mickleburgh 2008). Add to these difficulties ever-present concerns about terrorism, ranging from highly choreographed attacks involving multiple perpetrators to a single determined individual (the 'lone

wolf' scenario⁴), either of which could be potentially catastrophic, and one gets the sense of Olympics security as a complex high-stakes venture. One of our interviewees accentuated the enormity of this task by comparing Olympics security measures with the extensive security preparations that accompany a Super Bowl, suggesting that the Olympics is 'like holding the Super Bowl three times a day in ten different places for seventeen days.'

Managing these issues involves a deliberate emphasis on integrating disparate organizational parts around a common security objective. Organizational integration has become a standard feature of Olympic security operations. This emphasis is, loosely speaking, a key 'lesson learned' from the 1996 Atlanta Games that were marred by the explosion of a pipe bomb in Centennial Park. One of the

⁴ An intelligence assessment from Canada's Integrated Threat Assessment Centre identifies 'individuals inspired by a variety of ideological motivators or terrorist ideologies to conduct acts independently' as 'lone wolves.' The same report assesses the threat of a lone wolf attack at the 2010 Winter Games as low but conceivable, particularly if aimed at unofficial and peripheral targets (ITAC 2008).

dominant themes of an extensive post-Games analysis of Atlanta's security preparations conducted by Buntin (2000a; 2000b; 2000c) is that the Olympic Security Support Group (OSSG), the lead agency initially charged with the task of planning security for the 1996 Games, was plagued from the outset by, amongst other things, unclear jurisdictional issues running from county to state and federal levels, vague allocation of responsibility and financial commitment agreements amongst policing agencies and the Atlanta Committee for the Olympic Games (ACOG), and communication capabilities that were diminished by organizational and technical problems. The state governor eventually replaced the ineffective OSSG with the State Olympic Law Enforcement Command (SOLEC) and vested it with the legal authority to mobilize and deploy all of Georgia's public safety resources for the Olympic Games, with the exception of the Atlanta Police Department (Buntin 2000b: 3). However, SOLEC was created only eight months prior of the start of the Games and could never quite unify the fragmented efforts of the OSSG. Not including the Atlanta Police Department within the organizational structure of SOLEC also proved to be a crucial mistake, as communication delays between

Atlanta's 911 call centre, which received the bomb threat, and the state troopers responsible for policing Centennial Park (under command of the SOLEC), helped delay the evacuation of Centennial Park (Buntin 2000c).

Buntin made few recommendations in his exhaustive post-mortem but the lessons from his analysis are unambiguous: a strong organizational structure with clear roles and responsibilities paired with open lines of communication – literally as well as organizationally – are crucial to successfully managing the task of public safety at the Olympics (or any other large, significant, and non-routine event). 'The Atlanta experience' has since become synonymous with these organizational difficulties and is used as shorthand to identify the type of planning model that should be avoided.

Subsequent Olympic host countries have sought to establish early in the planning process well-defined central coordination units within the relevant policing agencies that are responsible for all Olympic-related security planning and to ensure they have clearly defined roles and responsibilities.⁵ In Salt

⁵ In Sydney this unit was the Olympic Security Command Centre (OSCC) within the New South Wales Police Force; in 2002 Salt Lake City the Utah Olympic Public

Lake City, the Olympic host that is most comparable to Vancouver in organizational terms, this was the Utah Olympic Public Safety Command (UOPSC). Federal agencies were coordinated by the US government by designating the 2002 Games a National Special Security Event, a designation that made the US Secret Service (USSS) responsible as the lead federal agency for developing and implementing security plans (in conjunction with local authorities), placed the FBI in charge of intelligence and threat assessments, and tasked the Department of Homeland Security with primary federal responsibilities for consequence management.⁶ The Major Events Division within the USSS, in turn, employs an organizational template that further specifies how federal agencies interact with one another (Reese 2008). At the state level special legislation was passed that

Safety Command (UOPSC); in 2004 Athens the Olympic Games Security Division (OGSD) within the Greek Ministry of Public Order; in 2006 Turin the Safety and Security Committee (SSC); in London 2012 the Olympic Security Directorate (OSD) within the London Metropolitan Police.

⁶ The NSEE designation was initially intended for presidential appearances and political summits but was applied for the first time for a sporting event for the 2002 Salt Lake City Winter Olympics and the February 2002 Super Bowl. All Super Bowls since 2002 have been declared NSSEs (Reese 2008). The Olympics were declared an NSSE prior to 9/11 in order to avoid the problems that plagued Atlanta's planning, not as a result of 9/11.

created the basis for state public safety agencies to work together with federal agencies and form UOPSC.

Canada's organizational structure for the 2010 Vancouver Olympics is similar to how the US approached the 2002 Games. The 2010 Games have been declared a 'major event' by the Minister of Public Safety, a designation that applies to any event of national or international significance where the overall responsibility for security rests with the federal government of Canada. This designation automatically makes the RCMP the lead agency responsible for developing and implementing all security plans for the designated event in conjunction with local authorities. The Major Event and Protective Services Division within the RCMP, in turn, employs a major event template similar to that used by the USSS to outline strategic principles, define roles and responsibilities, and streamline organizational communications within an overall command structure.

The template places operational planning as the responsibility of a Unified Command Centre, which in the case of the 2010 Winter Games is the Vancouver 2010 Integrated Security Unit (V2010-ISU). The V2010-ISU is composed of (but not limited to) the RCMP, VANOC

representatives, and representatives of the bylaw and law enforcement agencies of Vancouver, West Vancouver, Whistler, and Richmond. Federal partners include the Department of National Defence, Public Safety Canada, Transport Canada, the Canadian Air Transportation Security Agency, and Citizenship and Immigration Canada, amongst others.⁷ Department of National Defence operations are coordinated through Joint Task Force Games (JTFG), a unified command group working out of the Canadian Forces base in Esquimalt, BC, in what military officials have dubbed 'Operation Podium.' Intelligence and risk assessments are provided to the ISU by Canada's Integrated Threat Assessment Centre (ITAC), a unit within the Canadian Security and Intelligence Service (CSIS), working in conjunction with the RCMP's Joint Intelligence Group (JIG), an intelligence unit created for the specific task of monitoring Olympics risks and threats. Provincial efforts in the

⁷ All of the federal agencies on the ISU are: Public Safety Canada, 2010 Winter Games Federal Secretariat, Department of Foreign Affairs Canada, Department of National Defence, Citizenship and Immigration Canada, Transport Canada, Canadian Air Transportation Security Agency, Privy Council Office, Department of Fisheries and Oceans, Public Work and Government Services Canada, Patrimoine Canadian Heritage, Indian and Northern Affairs Canada.

realm of public safety for 2010 are channelled through the British Columbia Public Safety Unit (BC-IPSU), which consists of provincial officials who have expertise in disaster management, emergency planning, and public health. The BC-IPSU is physically co-located with the V2010-ISU, representing in part the desire for integrated planning on multiple governmental levels.

The V2010-ISU is a temporary unit but will likely have effects that last beyond February 2010. One way these effects will extend is through the development of the Major Events Template itself. There is already significant formal and tacit RCMP expertise in major event security, but the magnitude of the Games makes it an unparalleled opportunity to further develop this expertise for public events. The funding structure and international profile of the Olympics makes it an anomaly that is not likely to be duplicated in the near future, but it nonetheless offers an opportunity to more fully develop the Major Events Template in ways that will influence how future public events in Canada are managed.

More significantly, the Games offer an opportunity to develop public safety provision within BC and between BC and Washington state. A good indicator of the

lessons Olympics security may yield for public safety can be found in the report of a post-2002 Winter Games security debriefing conference (Oquirrh Institute 2002). A central theme amongst the seven lessons identified in that report is the importance of good communication processes within and between public safety agencies. Good communication processes, in turn, were seen to rely upon organizational clarity, technical capability, but most importantly upon 'the sociology of human relationships' (2002: 20). That is, while strong formal structures are needed to enable different agencies to work together to meet the needs of the event and public safety in general, workable relationships built on reciprocal trust are the 'mortar' that makes such structures truly integrated in that they can overcome inter-agency divisions and rivalries that tend to hamper the flow of information (Decker *et al.* 2005; Bellavita 2007).

Many individuals we have spoken with in our research indicate that the development of this type of social capital and subsequent inter-organizational integration and increased information sharing would be a significant legacy of the 2010 Winter Olympics. The creation of the BC-IPSU for example not only indicates structural integration

but the fact that it is co-located within the V2010-ISU provides opportunities to develop relationships with the RCMP and within the BC-IPSU that will last beyond the Games. Integrated alignment between public and private agencies may also be fostered by the operational requirements of the Games.

Critical infrastructure protection (CIP) is one domain where this integration is particularly evident. CIP is a key component to major event security and public safety more generally. Despite this centrality, effective CIP plans can be hampered because the majority of critical infrastructure assets (such as telecommunications networks) are privately owned; one emergency management official we spoke with estimated that 80-90% of Canada's critical infrastructure is owned by the private sector. This presents a security challenge because corporations are often reluctant to share information with government for many reasons, one of which is because as a general rule once information is shared with government it can become public under Access to Information provisions. Corporations see this as undesirable because they fear that such publicity can result in losing control of trade secrets.

Restricted information flow limits the effectiveness of CIP plans, particularly in light of how much critical infrastructure lies beyond the informational domain of government. Communications continuity cannot be provided for if, for example, emergency planners do not know where crucial but privately owned network stations are located. However, the same emergency management official noted above remarked that these barriers were being minimized in the lead up to the Games.

Another significant organizational legacy of the 2010 Olympics may be the deepening of cross-border cooperation on large-scale emergencies, border security, and counter-terrorism. The United States is keenly interested in security preparations for the 2010 Olympics given Vancouver's proximity to the US. This interest is reflected in the creation of the US 2010 Olympic Security Committee (the US equivalent of the V2010-ISU) and an integrated Multi-Agency Coordination Centre (MACC) in Blaine, Washington, comprised of representatives from US federal, state, and local law enforcement agencies, military representatives, emergency response agencies, and various liaisons from Canadian agencies. Reports suggest that the US 2010

Security Committee (USSC) has turned to exploring legislative and/or protocol changes needed to enable US involvement in the management of cross-border issues that might arise during the Games (Morgan 2007). The details of this harmonization are difficult to ascertain, but a report from the USSC indicates the general areas where the US is focusing their efforts: integrating federal, state, and local security operations, consolidating security emergency operations for US response efforts (both of which are evidenced by the MACC), harmonizing bi-national standard operating procedures for crisis response, and facilitating legitimate cross-border travel while minimizing illegal trafficking (Larson 2008).

The issues outline in the USSC report are not unique to the Games, of course, but have emerged as central concerns for policymakers on both sides of the border since 9/11. Indeed, the aims of the USSC resemble a distilled version of the *Security and Prosperity Partnership* mandate agreed upon by Canada, the US, and Mexico to 'establish a common approach to security to protect North America from external threats, prevent and respond to threats within North America, and further streamline the secure and efficient movement of legitimate, low-risk traffic across our shared borders'

(DHS 2005). This resemblance indicates how security for the Olympics does not exist apart from but instead serves to intensify wider security concerns. The 2010 Olympics provides an opportunity to advance cross-border cooperation on issues that, while germane to the Olympics, are also relevant to the ongoing harmonization of security policies between Canada and the United States. As one Washington state official said in regards to the efforts of the USSC to integrate public safety in Washington, 'we need this regardless of the 2010 Olympics, but [the Games] heightens the need' (Taylor 2008).

Precedent for this type of event-catalyzed harmonization can be found in the example of operation 'Shiprider' used for the 2006 Detroit Super Bowl. 'Shiprider' is a colloquial term for Integrated Marine Security Operations (IMSO), a cross-border initiative between the RCMP and US Coast Guard to cooperatively police shared seaways as set out in the *Security and Prosperity Partnership*. IMSO allows for RCMP officers to be placed on US Coast Guard watercraft and vice versa in order to conduct cross-border law enforcement operations. The project was pilot tested in 2005 through a series of exercises and put into 'live' use for the first

time to police the Detroit River and surrounding waterways during the 2006 Super Bowl in Detroit. This operation became the basis for further development and expansion of such practices throughout the Great Lakes region, St. Lawrence waterway, and the Vancouver Island/ Washington State border areas.

The harmonization of emergency response plans and communication protocols between public safety agencies is one organizational domain that has received attention in the run-up to the 2010 Games. Numerous large-scale public safety exercises have been undertaken to support the tri-partite aims of 'improved preparedness and ability to respond to any potential emergency during the Vancouver Olympics Games in 2010; ongoing and continual improvement in the federal government's ability to ensure the safety and security of Canadian's [sic] and Canada; [and] support for the Government of Canada's commitment to the Security and Prosperity Partnership' (PSEPC 2006). Upcoming exercises include TOPOFF 5, the fifth round of high-level public safety exercises involving top officials ('top-off') between participating countries. Notionally scheduled for April 2009, TOPOFF 5 will test response capabilities

amongst officials from Canada, the US, and Mexico in relation to 'terrorist events that could affect [the] 2010 Olympics.' Specific scenarios will not be disclosed, but previous TOPOFF rounds have focused on different types of chemical, biological, and radiological attacks. These exercises are in addition to the specific exercises being conducted by the V2010-ISU, which have included a 'bronze' level table-top exercise in November 2008, a silver level exercise dubbed 'Pegasus Guardian 2.2,' involving the deployment of military air and sea crafts out of the Canadian Forces Base in Esquimalt, BC in February 2009, and culminating in 'gold' level exercises scheduled for late 2009.

Facilitating the smooth entry of legitimate travellers at the border while minimizing the flow of unwelcome people and illegal goods is a wider concern made more pressing in advance of the large numbers of people who will be crossing the border in February 2010. An official with the Canadian Border Services Agency recently stated that the CBSA is 'not expecting major problems for the Olympics' such that they would have to modify existing procedures, a view that both BC and Washington officials sharply dismissed (Inwood 2008a; Lee 2008a; Paperny 2008). Keenly

aware that long waiting times at border crossing may translate into lost economic opportunities, attention has turned to facilitating cross-border movement within the confines set out by the US Western Hemisphere Travel Initiative that requires all persons entering the US to carry a passport or other acceptable documentation.

Pursuant of its mandate to shape border security policy and implementation strategies, the Pacific North West Economic Region Council (PNWER) has been advocating for new or expanded initiatives in this regard, including the development of more technologies for pre-clearance and processing prior to physical arrival at the border, new online systems to streamline customs and duty declarations and payments, and the further development of pre-clearance procedures for train services between Vancouver and Seattle (PNWER 2008). Ultimately, the PNWER sees these recommendations as part of an 'unparalleled opportunity to leave a positive legacy, creating a new vision for a border that is protective and convenient' long after 2010 (PNWER 2008). These suggestions have been favorably received by the BC Solicitor General who stated that the PNWER recommendations would 'lay out our agenda' for

the following year (Inwood 2008a).

These proposed measures would also further fuel an already insatiable need for the types of personal data that are required in order to fulfill the informational requirements of the risk profiles upon which these initiatives are based. These informational requirements, in turn, foster an environment where new information processing technologies are continually deemed to be warranted or where existing technologies are repeatedly enhanced to meet ever-expanding informational requirements. This process of expansion resembles a form of 'function creep' where practices and technologies that were initially established exclusively for one purpose rapidly expand into new domains and find new uses. Enhanced drivers' licences with embedded radio frequency identification (RFID) chips, for example, were recently introduced in BC as a way to meet the demands of the US Western Hemisphere Travel Initiative. Supporters of this initiative assured critics that they would not pose any threat to personal privacy, but as has been recently argued in the *Toronto Star* (Clement & Bennett

2008) there will likely be pressures to use RFID capabilities far beyond their initially-proposed uses and settings as they are adopted by more jurisdictions. The exceptional demands of Olympic security will likely continue to fuel such expansionist pressures. PNWER, for example, explicitly includes 'expansion of enhanced drivers' license initiatives' as part of its raft of border security recommendations to policy makers (PNWER 2008: 4). What this might look like in practice can only be speculated upon, and the mere presence of the technology does not guarantee that such expansions will occur. Nonetheless, calls to exploit RFID-enabled EDLs may ultimately serve as a model or reference case for the rest of Canada.

Finally, it should be noted that part of the organizational structure for the Games will include 25,000 ordinary citizens who are expected to volunteer to help out in assorted capacities. Such participation promises to produce lasting memories that could be one of the more positive legacies of the Games. Potential volunteers just need to be willing to dedicate their time, and also pass an RCMP background check.

The Business of Olympic Security

In the fall of 2008 we attended a workshop on sports event security where one of the speakers began his talk by wryly observing that 'The Olympics aren't just about big business any more.' This was a rather telling statement, and not simply because he did not even mention sports as being an integral component of the Games.

Instead, in trying to accentuate how security has become a major consideration for mega event planners, he ignored the fact that security for mega events is itself now already a large business.

September 11th 2001 dramatically escalated the financial resources devoted to Olympic security. By way of establishing a benchmark, approximately \$180 million USD was spent on security for the 2000 Sydney Summer Olympics. In comparison, and despite the fact that the winter Olympics are smaller than the summer Games by about half, almost \$310 million USD was spent on security for the 2002 Salt Lake Winter Olympics. The Greek government dramatically eclipsed previous figures by spending an estimated \$1.5 billion USD on security. Estimates for the 2006 Torino Winter Games put security costs

at approximately \$400 million USD when the substantial military costs were factored in. Officially, China spent \$300 million USD on security for the 2008 Summer Games, a figure that does not include massive security expenditures contained in other budgets (Thompson 2008).

The security budget for the 2010 Vancouver Winter Games, originally pegged at \$175 million CAN at the time of the bid, was subsequently assessed by the Royal Canadian Mounted Police as being 'drastically low' (RCMP 2005). The Public Safety Minister indicated in late 2008 that a figure of \$1 billion for the security budget is about right, and in February 2009 the budget was confirmed to be \$900 million CAN (Curry & Friesen 2009).⁸ The London 2012 security budget is seeing escalations even steeper than

⁸ The 2010 security budget breaks down amongst federal agencies as follows (in millions CAN): 491.9m to the V2010-ISU, 212m to the Department of National Defence, 25m to Transport Canada/NAV Canada, 8.8m to Transport Canada, 11m to CSIS, 9.8 to Industry Canada, 1.2m to Citizenship and Immigration Canada, 1.2m to Public Safety Canada, 0.9m to Public Health Canada, 1.4m to the Federal Employee Benefit Plan, and 137m reserved for unforeseen contingencies.

Vancouver's. Set originally at £600 million GBP, the security budget for 2012 has been revised upwards twice: first in December 2007 to exceed £838 million GBP and again in October 2008 to £1.5 billion GBP (Sherman 2007; Merrick 2008).

These figures likely underestimate the full costs of Olympic security. First, the full cost of deploying military personnel and equipment, for example, or working hours contributed by government staff members on Olympic-related projects, may not be accurately reflected in Olympic security budgets. These invisible costs make it difficult for the public to acquire a full accounting of the true cost of Olympic security, a figure that is perhaps even unknown to the government itself. Second, costs for projects timed to coincide with the Olympics are not reflected in Olympic security budgets. Accentuating this point is the \$6.5 billion USD China funnelled into the *Grand Beijing Safeguard Sphere* between 2001 and 2008 that exists, in terms of financial accounting, outside of Olympic security spending. In the case of Vancouver, upgrades to the lower mainland's E-Comm centre or federal spending in the areas of public transit and maritime transportation security are not strictly speaking Olympic expenditures but have been

obviously timed to coincide with the 2010 Games.

Potential host cities must make elaborate promises regarding security provision that have been responsible in large part for some of the Olympic budget escalations that recent Games have exhibited. Future Olympic host cities may follow two apparently contradictory directions when it comes to security budgets, each of which is typified by current contenders for the 2016 Games. On the one hand we may witness further dramatic escalations in Olympic security budgets as potential hosts seek to guarantee security at ever-greater costs. Rio de Janeiro has recently disclosed a \$14.4 billion (US) budget for the 2016 Games, a figure almost equal to the combined budgets of the other three competitors. What makes this figure truly remarkable is that organizers state they already have most of the venues Rio de Janeiro would need to host the Games, thereby raising the question of just how much would be spent on security if venue construction is not the primary budget line. On the other hand security budgets may paradoxically fall as potential host cities make significant inward investments in their security infrastructures prior to making an Olympic bid in order to make itself marketable as a suitable host city, thereby

increasing competitiveness while at the same time wiping significant amounts from later budgets. This appears to be Chicago's tactic to bolster its 2016 bid by investing in *Virtual Shield*, an elaborate network of integrated law enforcement and private sector surveillance cameras that blanket everything inside of the Loop and which, not accidentally, employs face recognition technology first developed by IBM for the 2008 Beijing Games. In such a scenario, the security 'legacy' may come to precede the event itself.

One reason why it is worth keeping these large figures for Games security in mind is that the amounts of money dedicated to security can be a key factor in determining the degree and intensity of security-related surveillance measures. In an environment where security risks are always present, but are also almost impossible to quantify or establish with any degree of precision, almost any security measure can be sold as a precautionary 'just in case' measure that is needed to mitigate—so some unknown degree—the possibility of a catastrophe. Indeed, the authoritative *Jane's Intelligence Review* (2007) cautions about the embrace of what it refers to as 'high consequence aversion' where 'event organizers will

allow potential worst cases to drive costly and inappropriate security measures.' This was also a point one of our interviewees—an extremely high figure who has ultimate authority for the security preparations for one of the world's largest mega-events—explicitly confirmed when we asked him how he established the real world parameters on the level and extent of security measures they would deploy. His response was 'that's dictated by your budget.' If this is indeed the case, and security budgets continue to be driven by the spectre of the worst case scenario, we can expect to see the continual expansion of intensive security measures both at the Games and in their aftermath.

The point here is not to enter the debates about whether these costs are justified or if projects timed to coincide with the Games should or should not be included as Olympic expenditures, but instead to accentuate how security has emerged in the 9/11 environment as a multi-billion dollar industry, one that is so enormous that it is increasingly characterized as a 'security-industrial complex' (Whitaker 2006). And while the security preparations of the Olympics only accounts for a fraction of global security budgets, the sums spent on the Games are still

considerable. Moreover, sports mega-events are an important niche in the wider economy and marketplace for security.

Large, multinational military aerospace and national defence contractors are increasingly drawn in to the business of Olympic security preparations. This attraction is only in part due to the financial sums involved; while the contact with Greece to provide an extensive surveillance and communications network for the 2004 Games was worth an estimated \$322 million USD for Science Applications International Corporation (SAIC), this is a relatively small sum for this San Diego-based aerospace and defence contracting firm given that it has posted annual revenues of between 7 and 8 billion USD in recent years.

The competition for Olympic security contracts also arises in large part because they provide high-profile opportunities to showcase new technologies, develop core strengths in expanding areas, crack into expanding domestic and foreign markets, and secure long-term 'legacy' contracts in a context where 'homeland security' markets have dramatically expanded since 9/11 (Dao 2002). In this context, the Olympics are a singular occasion in a wider field of domestic

security wherein 'high technology companies are wooing willing governments with their security and surveillance products designed to detect "terrorists" and also other miscreants who may be found in cities or in airports and at borders' (Lyon 2004: 136).

The corporations involved in the 2004 Athens Olympics, for example, used their involvement as a platform to advertise their capabilities. SAIC's success in securing the 2004 Olympic contract was due in large part to its success in marketing their previous involvement in the 1996 and 2002 Olympics. SAIC also emphasized that it had the 'brain power' to handle the project; immediately after the 2002 Salt Lake Games SAIC hired David Tubbs, a 24 year veteran of the FBI and executive director of the Utah Olympic Public Safety Command, and appointed him as manager of SAIC's Justice Information Systems Group where he was instrumental in securing the contract over the leading competing consortium lead by Lockheed Martin.

SAIC has identified systems integration as one of its key growth areas for the future and marketed their involvement in security for the 2004 Olympics as a stepping-stone towards larger and more complex integration work for the US

government and, eventually, aims to position itself as the preferred contractor for these types of services (Finnegan 2005). Siemens, a contributing member of the SAIC-led consortium in Greece, currently markets its 'proven experience' at the 2004 Games in order to position itself as the lead systems integrator for the 2012 Olympics (Siemens 2006).

While China handled security preparations largely 'in house' with little outside assistance (though Interpol supplied some intelligence), they used the Olympics as an opportunity to stock up on cutting edge surveillance equipment. Western technology firms, on the other hand, are eager to enter the Chinese surveillance market, which the *New York Times* estimates will be worth more than \$43 billion USD by 2010 (Bradsher 2007a). In a market analysis report produced before the Beijing Games, the Security Industry Association advised its members that the Games and the wider *Grand Beijing Safeguard Sphere* would offer 'huge commercial opportunities' and a chance to 'showcase world-class security technologies and services' to the Chinese government (SIA 2007: 26). The SIA also advised members that the 2008 Games might offer opportunities for long-term maintenance contracts and could

also help secure contracts to other high-profile events in China such as the 2010 World Exposition in Shanghai and the 2010 Asia Games in Guangzhou. Some of the major corporate players that supplied surveillance technologies to China include IBM, Panasonic, Honeywell, Siemens, and Sony, which raises not only ethical questions about supplying surveillance technologies to an authoritarian state but legal question of whether US-based companies broke post-Tiananmen Square trade rules regarding supplying the regime with crime control equipment (Bradsher 2007c, 2008).

The details of who is supplying what technologies for the 2010 Winter Olympics are guarded and will likely not be known until after the Games. However, companies such as SAIC, Raytheon, Siemens, and Thales Systems have approached the government with proposals for security services that are likely similar to their past involvement as system integrators for previous host cities. Regardless of who supplies these technologies, each Olympics can be seen as a leading edge showcase of security technologies, some of which eventually trickle out into wider society beyond the Games. Some of these technologies are examined in the next section.

Technology and Technological Integration

While the international security industry offers products and services that extend to such things as weapons, private security officers and safety vests, the major trend in security for the Games has been the use of assorted information, communication and visualization technologies. This is in keeping with the wider embrace of high-tech surveillance measures as a technical 'fix' for terrorism concerns since 9/11 (Ball & Webster 2003; Lyon 2003; Haggerty & Ericson 2006). Though the specific technologies deployed for each Olympics varies widely, one commonality is that the Games provide a strong incentive to integrate discrete surveillance technologies into comprehensive networks. These integrated networks can not only produce a remarkable visualizing capacity to be deployed during the course of the games, but can also mark a long-term step-change in the surveillance infrastructure of the host city.

The 2004 Athens Summer Games, for example, were characterized by a surveillance blanket that encompassed three dozen competitive venues and 6

official non-competitive sites spread across Athens and 4 other co-hosting cities as well as a large part of central Athens where peripheral events were held. Approximately 50,000 security personnel were deployed for the Games who blended with cutting-edge surveillance technologies. Most conspicuous amongst these technologies was an overhead blimp that circled the main Olympic venues for up to 16 hours a day. In addition to being equipped with television equipment, the blimp was fitted with two military-grade electro-optical and infra-red cameras, a high-resolution, zoom-enabled visual camera, three digital recorders (for recording flight data and on-board operations), a GPS locating system integrated with a GIS street mapping system, and a digitally encrypted downlink to supply images and data to the Olympic Security Command Centre.

In Greece, NATO supplied and operated an Airborne Early Warning and Control System (AWACS) aircraft to patrol restricted airspace zones. NATO also patrolled the port of Piraeus with sonar equipment where

seven cruise ships providing temporary hotel accommodations were docked. Scanners capable of detecting chemical, biological, radiological, and nuclear devices scanned all vehicles entering specified security rings. A double-layered fence equipped with motion detecting sensors surrounded the athlete's village and over 1,500 temporary CCTV cameras were installed around the central Olympic venues; in the main Olympic plaza this amounted to one camera every 50 meters. These cameras were in addition to the nearly 400 being phased in at the city's new airport in time for 2004, the 200 cameras already in operation in the city's public transit system, the 220 (up from 48 for the Games) in the central business and entertainment areas, and 200 in the port of Piraeus (Samatas 2004: 116).

The centrepiece of the Greek security and surveillance blanket was an extensive digital communications backbone supplied by a consortium of technology firms lead by SAIC. This system, known in military parlance as a C4I network for 'command, control, communications, coordination, and intelligence,' aimed to solve a problem endemic in the information age. While innovative new technologies (including surveillance

technologies) provide ever more ways to generate data and visualize the external world, this proliferation of new devices also creates the two-fold problem of how to manage all the information they produce and how to use disparate technologies in a complementary manner.

The C4I system was designed to solve these problems by integrating the range of surveillance assets and computer-aided planning systems (67 subsystems in total including vehicle locating and tracking systems, CCTV sub-networks, perimeter monitoring systems, the airborne surveillance unit), routing data through numerous subcommand centers and five mobile subcommand centers where it could be filtered, and centralized in a single central command center. The system was also intended to provide secure communications between the command centre and field personnel through a secure digital trunk radio network consisting of 23,000 terminals. As such, the C4I system is a microcosm of wider tendencies in the field of security, most notably the desire for the seamless integration of technological, informational and human capabilities in a unified whole in order to hopefully

anticipate, detect, and respond to security issues.

While SAIC's system was delivered to meet the needs of the Games, from the outset it was intended for long-term use afterward as part of a broader modernization of the Greek law enforcement and public safety technical infrastructure. Not all components of the Olympic security blanket remained after the Games, of course; the surveillance blimp, for example, was stripped of its equipment and returned to the Swiss company from which it was on loan, although it is an open question as to how all of the equipment contained in the blimp was subsequently deployed. Nonetheless, the central command centre and C4I network remained for post-Games coordination of fire, ambulance, traffic, and public safety with SAIC providing system integration logistical support until 2013 (SAIC 2008). Of the 1,500 'temporary' CCTV cameras installed for the Games approximately 400 were retained for post-Games use over and above the increased CCTV prevalence at other sites such as airports and major highway corridors that were prompted by the Games (Samatas 2007).

These investments in technology, in conjunction with other skills-building opportunities, were an

explicit component of Greece's Olympic legacy. George Floridis, Greece's Minister of Public Safety, said of the \$1.5 billion USD Greece invested in security for the Games: 'This great expenditure, however, is not concerned only with the duration of the Olympics. It is an investment for the future. The special training, technical know-how, and ultramodern equipment will turn the Hellenic Police into one of the best and most professional in the world, for the benefit of the Greek people' (Floridis 2004; 4). Indeed, Greece expected the Olympics to provide the opportunity to transform itself into a counter-terrorism 'superpower' that could export its newly-developed expertise to other countries (Murphy 2004).

Security for the Beijing Games followed a similar pattern of weaving cutting-edge technologies into a cohesive blanket of human and technological surveillance. The monitoring of venues and visitors was conducted by nearly 100,000 law enforcement staff drawn from local police (~40,000) and armed forces (~30,000) with the balance consisting of paid and unpaid civilian security guards/volunteers. In the surrounding cities a 300,000-strong contingent of 'community security volunteers' informed

local authorities of anything suspicious (Thompson 2008).

The surveillance technologies deployed in China were equally grand, though specifics are not as readily available as for Athens due to the fact that the 2008 Games are relatively recent and China's closed government makes learning the specifics exceedingly difficult. That said, we know that 300,000 CCTV cameras, some of which pilot tested new facial recognition software, were reportedly installed in Beijing in time for the Games in what has been described as the largest, most comprehensive CCTV network ever (Wong & Bradsher 2008). Like in Athens, devices were used to scan vehicles entering certain zones of the city for chemical, biological, radiological, or nuclear substances.

The estimated 15 million tickets sold for the Chinese Olympic events were embedded with RFID chips, ostensibly to prevent ticket counterfeiting. The tickets themselves were said not to carry any personal information aside from an identifying serial number. However, a ticket's serial number was connected to databases detailing information about the ticket holder including their name, address, passport number, telephone, and email address; information that individuals had to provide when

purchasing a ticket. This use of RFID technology obviously enabled anyone with an appropriate reading device to engage in surreptitious close-range identification of any person possessing a ticket, irrespective of whether they were close to an Olympic venue or not. Technology watchers have hailed this use of RFID technology as the first major test of this kind of adaptation of the technology that, if successful, will be a significant boost for the wider use of RFID-enabled tickets and identity documents.

Some of the other notable surveillance-related developments introduced in Beijing in the context of the Olympics include fitting taxis with listening devices integrated with GPS locating systems that could be monitored from central command centres in the name of 'driver safety.' Hotels popular with foreign visitors were also suspected of being bugged by audio and video feeds to such an extent that the US State Department issued a statement that 'all visitors [to China] should be aware that they have no reasonable expectation of privacy in public or private locations' (Oster & Fairclough 2008). The need for this warning was accentuated later in 2008 when a Danish soccer team competing in a FIFA match in China discovered that two men

in an adjoining hotel room were monitoring their team meetings through a one-way glass (Maginer 2008).

Beijing's surveillance blanket was also wrapped in a broader modernization process under the banner of *Golden Shield*, a series of 'golden' projects initiated in 1998 to upgrade and expand China's national digital information and telecommunications infrastructure (Walton 2001).⁹ Most media attention has focused on China's efforts to shape and block internet traffic inside the country, efforts that have been nicknamed the 'Great Firewall of China.' Golden Shield also includes, according to a prominent report on the project, 'a nationwide digital surveillance network, linking national, regional and local security agencies within a panoptic web of surveillance' (Walton 2001: 16).

China's *Safe City* project advances this goal by developing the surveillance infrastructure of 660 cities. In Shenzhen, for example, where police officers already carry GPS units integrated with central command mapping systems and 20,000 CCTV cameras have recently been installed, migrants

are required to carry residency cards that include digital records of their name, address, work history, educational background, religion, ethnicity, police record, medical insurance status, landlord's phone number, and possibly personal reproductive history (in order to enforce China's one child policy). Plans are being studied to add to these cards details of a person's credit history, subway travel payments and small purchases they charged to the card. All migrants to Shenzhen who do not have permanent residency cards are required to carry such ID cards; a population which amounts to 10.5 of Shenzhen's 12.4 million inhabitants (Bradsher 2007b). Beijing's Olympic security efforts were nested in a similar *Safe Cities* project named the *Grand Beijing Safeguard Sphere*, a \$6.5 billion USD investment into Beijing's surveillance infrastructure which human rights advocates have denounced as providing a legacy of invasive surveillance with manifold possibilities for misuse (China Rights Forum 2006).

The integration of surveillance technologies is also at play in London's preparations for 2012. Unlike Athens and Beijing, London already has a highly advanced public safety infrastructure. This shifts the emphasis from building integrated networks from

⁹ Including Golden Bridge, Golden Gate, Golden Car, Golden Sea, and Golden Macro, amongst others (Walton 2001: 17).

scratch to leveraging existing systems and capabilities into cohesive networks. London is home to the greatest concentration of CCTV cameras in the world (although Beijing may now claim this title), but the London cameras are a patchwork of systems operated by private networks and various governmental authorities that, as yet, do not resemble an all-inclusive network. The London Metropolitan Police has announced it plans to explore how 'the current capabilities of various CCTV networks might be harnessed and integrated in London within the current legislative framework to deliver greater effect in mitigating specific threats as part of the Olympic security effort,' according to Tarique Ghaffer, former Assistant Commissioner and chief of the Olympic Security Directorate (BBC 2008).

The Met has turned to EADS, a UK aerospace and defence contractor to develop and implement the technical requirements that will allow the Met to tap into CCTV systems that are beyond its own network, such as those operated by Transport for London, private businesses, and traffic monitoring cameras, and incorporate them as extensions to their own CCTV capabilities. This would effectively boost the Met's CCTV network to 500,000

cameras. EADS is also contracted to build a central command centre in London where this can all be monitored (O'Connor & Sherman 2008). EADS, in turn, hopes to move beyond CCTV integration to provide system-wide integration services for the Olympic Security Directorate and other stakeholder agencies before and beyond 2012 (Baker 2009). The British Transport Police (BTP) is planning similar forms of systems integration. These plans revolve around developing a geographic information system (GIS) that will consolidate geospatial information spread across various sources including the BTP's own files and open-source information, and will be able to sort this information according to relevance to defined locations, and display that information through a map-based visualization tool.

Face and hand-scanning technology is being used to identify construction workers entering and exiting the Docklands Olympic constructions site and, if deemed successful, may be used to identify ticketholders entering Olympic venues in 2012. Another surveillance measure that is being justified in the contexts of the London Olympics is a proposal to expand the national DNA database by allowing

familial DNA identification (O'Connor & Sherman 2008).

All of these developments provide a sense of the emergence of a totally integrated and seamless surveillance web. That is certainly the ambition of many authorities, and things are undeniably moving in that direction (Haggerty & Ericson 2000). Nonetheless, the dream of total system integration at this point remains the stuff of Hollywood fiction. A number of factors complicate the effectiveness of these efforts and raise their own risks.

The technical logistics of system integration can still be beyond the grasp of current computational capabilities. The C4I system in Athens, for example, did not work to expectations during the 2004 Olympics. The Command Decision Support System (CDSS) at the heart of the C4I network, and which was the actual engine of integration, performed poorly and was reportedly full of technical glitches that severely limited its functional capacity. Most of the network's subsystems worked as intended, but 'the controlling hub of the C4I network was absent' (Samatas 2007: 229). This was partly due to the fact that many venues were not completed on time, leaving less time to fit up the network before the start of

the Games, but also due to the fact that the CDSS had to process and shuttle massive amounts of data that may have been simply beyond the capacity of the software to manage (Samatas 2007). Rapid advances in computational power make it foreseeable that this problem will be significantly reduced in the future. It is also equally foreseeable that the amount of data to be processed will also increase at an equal or greater rate, again outpacing the ability for intelligence to be effectively integrated into security systems (van Creveld 1991).

A different sort of technical obstacle is illustrated by the London 2012 preparations. Leveraging existing surveillance capabilities is obviously preferable for authorities on a budget than building entirely new and expensive networks, yet integrating these capabilities faces challenges related to interoperability. Systems simply cannot be integrated if proprietary specifications do not allow them to be programmed to 'speak' to one another. While this has been a recurring obstacle in trying to join-up systems, in the future it might be overcome as more surveillance systems are built as commercial off-the-shelf (COTS) applications that comply with industry-wide standards rather than proprietary standards, thus allowing a

theoretically infinite daisy chain of integrated, interoperable systems. The geospatial system being developed for the BTP outlined above, for example, complies with the standards of the Open Geospatial Consortium and International Organization for Standardization (OGC/ISO) rather than proprietary standards, raising the prospect that this system could be integrated with others using the same standard.

While solutions to the above-noted problems are foreseeable, system integration raises the more fundamental problem of system complexity (Perrow 1999). The integration of individual systems makes the complexity of the system as a whole greater than the sum of its parts. As system complexity increases, so do the chances of producing unexpected, nonlinear interactions and, consequently, system failure. Such failures can be difficult to diagnose as they rarely have a single source but are, as noted, the outcome of unintended interactions. Additionally, tightly coupled subcomponents ensure that any failure is passed on to other linked systems, further obfuscating diagnosis while raising the possibility of system-wide failure. Technological solutions to the problem of complexity may be sought, but such solutions paradoxically

tend to increase a system's complexity, not reduce it, and therefore contribute to rather than minimize the problem. Ultimately, the only solution to the problem of system complexity is modularity; breaking down complex systems into manageable, firewalled parts, thereby reducing the complexity of the whole (Perrow 2008). Modularity is the exact opposite of where contemporary technologically-driven security solutions are going.

Such concerns have not dampened official enthusiasm for high-technology Olympic security. Indeed, Chicago's Mayor Daley, looking ahead at the prospect of landing the 2016 Olympics, recently issued what some might see as the simultaneously reassuring and disconcerting claim that 'security and terrorism won't be an issue if his Olympic dreams come true because, by 2016, there will be a surveillance camera on every street corner in Chicago' (Spielman 2009).

While it is beyond the purview of our report to evaluate the likely successes of such surveillance techno-solutions to the problems of Olympic security, it is worth at least mentioning the issue of displacement as it pertains to the prospect of an ongoing physical expansion of surveillance measures. In criminology,

displacement refers for the tendency for anti-crime efforts to simply move a crime problem to another location. There is a sense in which terrorist displacement could be one unintended consequence of intensive Olympic security measures. Security can certainly reduce (but not eliminate) the prospect that a terrorist will successfully attack one of the premier Olympic attractions. And while terrorists would ostensibly prefer to target a symbolically loaded event such as the opening ceremonies, if heightened security makes that impossible, then there is the real prospect that they could simply attack other proximate targets that are less secure – what is generally referred to as a ‘soft target’ approach. The massive media presence at the Olympics ensures that their actions will reach a global audience irrespective of the target. This is not an argument against security measures, but it does point to an irresolvable tactical dilemma when trying to deal with dedicated terrorist groups.

Something of this sort occurred in Atlanta when Eric Rudolph chose to detonate a bomb at the Centennial Olympic Park during the 1996 Atlanta Olympics, a site which was considerably less secure than the main Olympic venues. One implicit strategy has been to try and identify such

‘soft’ targets and to then increase the security and surveillance measures at those sites. In doing so, however, planners also introduce an expansionist dynamic to surveillance practices where ever more locations and sites are seen to be in need of security and surveillance measures because they are not as secure as other more high profile targets. The issue here is that it is ultimately impossible to secure all of the potential ‘soft’ targets, and that attempting to do so introduces an amplifying spiral of security and surveillance measures that risks surrendering the very freedoms that officials hope to preserve.

Direct comparison between Canada’s security, safety and surveillance preparations for the 2010 Winter Games and any other site would be misleading. Most obviously, legal regimes differ widely amongst these countries; the efforts undertaken in Beijing are not an indicator of what will unfold in Vancouver. As well, the Athens and Beijing Olympic surveillance efforts were embedded within large-scale improvements to their law enforcement and public safety infrastructures. Highly-placed security planners we spoke with about these preparations described Greece and Athens as ‘greenfield sites,’ a phrase meant to underline the twofold point that each country was starting

from a low initial baseline of public safety capabilities and that many venues for the Games were newly constructed, thus allowing surveillance to be literally built into the venues, thereby lending them much more permanence.

Canada, in contrast, already has a highly developed public safety infrastructure, and many of the events for the 2010 Games are being held in existing venues, meaning that security technologies will be retrofitted, making it less likely that they will become permanent. Nonetheless, it seems clear that as a general rule the assorted challenges, risks and anxieties prompted by hosting the Olympics trigger a 'surveillance surge,' where surveillance technologies are adopted with less public debate than would usually be the case because such measures are perceived to be warranted responses to a set of exceptional circumstances (Wood, Konvitz, & Ball 2003: 141). Indeed, authorities recognize that the Olympics can provide a pretext to introduce forms of surveillance that they have long sought for various purposes, as the Games provide a context in which citizens appear more willing to accept the need for enhanced surveillance measures, some of which remain as permanent additions to the existing surveillance

infrastructure. One can get a glimpse of this process in operation from a revealing statement contained in a government memo entitled 'No. 10 Policy Working Group on Security, Crime and Justice, Technological Advances' which deals with on the expansion of the DNA database in the UK. In contemplating introducing this possibly controversial measure, the authors concluded that 'Increasing [public] support could be possible through the piloting of certain approaches in high-profile ways such as the London Olympics' (Hennessy & Leapman 2007). Here, then, is a straightforward example of officials strategically using the Olympics to legitimate surveillance measures which are ultimately being sought for other purposes.

The RCMP Vancouver 2010 Integrated Security Unit has released few details about security preparations for the Vancouver Winter Games but some statements and reports indicate directions that are broadly in line with how security was managed at previous events. Regarding questions pertaining to airspace closures, the V2010-ISU has stated that a 'scalable airspace management and protection plan built on existing infrastructure is under development and will be in place during Games time.' This air

coverage is being supplemented by a contract tendered by the federal government to develop a system to detect small, low altitude aircraft in the lower mainland/Vancouver Island region. The contract 'reflects the desire to evaluate the current state of commercial systems for rapid implementation into the field for events such as the 2010 Olympics' and is currently under development by Lockheed Martin and Thales Canada (Lee 2008b).

The Department of Defence is retrofitting 19 CH-146 Griffon helicopters with electro-optical/infrared (EO/IR) sensor systems under Project INGRESS (Interoperable Griffon Reconnaissance Escort Surveillance System). These helicopters are being used for combat operations in Afghanistan but can be made available for 2010 duty if requested by the V2010-ISU. High-resolution satellite photographs of the Vancouver region are scheduled to be taken between March 1 and April 30th 2009 in order to provide 'seamless and consistent air-photo coverage' for 'all agencies involved in emergency management and public safety related to 2010 Olympics and all future emergency and public safety events,' according to the contract documents (Inwood 2008b). There is also the

possibility that such overhead monitoring could be augmented by the use of Predator surveillance drones on loan from the American government – and manned by American military personnel. These drones are again most familiar from their combat role in Afghanistan and Iraq, but are now also being used to monitor the Canadian/American border in the region from Maine to Washington with the aid of infrared and high definition images. The prospect of using these drones at the Vancouver Olympics was raised by Juan Munoz-Torres, who is the spokesman for US Customs and Border Protection, who effectively offered them to Canadian authorities: 'If the RCMP or Canadian government believes they can make use of the aircraft for support during the Olympics we will be more than willing to provide it' (White 2009) – an offer that the American authorities do not regularly extend in relation to their high-tech surveillance equipment.

The V2010-ISU is also reportedly in the process of purchasing Safesite, a multi-threat detection system capable of identifying, according to the product specifications, chemical warfare agents, gamma radiation, and toxic atmosphere signals. Safesite is currently employed at the White House, Super Bowls,

and was used at the 2004 Athens Games (Lee 2008b).

Acquisition of a \$1.3 million CAD geospatial software system (with \$600,000 of annual maintenance costs) was under review by the Major Events Division in Ottawa in 2007, but few specifics regarding the system's capabilities nor whether it was finally purchased were released. CCTV cameras will undoubtedly be used around venues, the athlete's village, Olympic-sanctioned gathering places, and along the Sea-to-Sky highway from North Vancouver to Whistler. This could amount to over 100 sites, though few precise details are available on how many will be used.

VANOC has signed an agreement with Olympic sponsor Garrett Metal Detectors to supply 550 walk through metal detectors and 1,100 hand-held metal detector wands to be used at Olympic venues despite advice from a Turin Olympic organizing committee executive to 'throw away the mag-and-bag' (airport-style checks) as they provide only 'illusory security' and are 'completely useless' when it comes to detecting non-metallic materials that could be used to make explosive devices (Lee 2008c).

Whether or not these measures will stay in place after the 2010

Games has been the subject of much speculation in the Canadian media. The V2010-ISU has released a statement in response to this question indicating that 'disposal of the security equipment after the Games will comply with the Memorandum of Agreement between the Province of British Columbia and the Government of Canada,'¹⁰ the terms of which do not seem to preclude their remaining in place or being implemented in other domestic contexts. One option available to the RCMP is to roll any equipment it may acquire into the department's Major Events Inventory, a stockpile of equipment for the management of major events, until needed at a later date. This option seems less likely for technologically sophisticated equipment whose shelf life is limited by the pace of technological advancement. In cases where obsolescence is a concern, there will likely be pressures for the immediate and continued use of the equipment, either in place in the Vancouver region or by distributing it

¹⁰ The V2010-ISU statement cites Section 3.03 of the 2006 Memorandum of Understanding between the federal government and B.C., which states: 'The parties agree that assets acquired for policing and security operations and services that are funded under this Agreement will be divided on an equal basis between them in accordance with the plan established by the Security Committee.'

across the department for other uses.

Emergency management during the 2010 Games will be coordinated from the existing E-Comm centre in East Vancouver. This centre, and the wider emergency management system that it coordinates, are already highly developed but improvements are being made in anticipation of 2010. The Director of Emergency Management at the E-Comm centre indicated to us that the centre would be undergoing a gap analysis in 10 key areas in order to identify potential weaknesses. Consistent with the notion that the Olympics provides a broad catalyst for public safety improvement, he also indicated that this reflexive analysis was to be conducted anyways but has been motivated at this time by the coming 2010 Games. As well, the Director indicated that some of these improvements will be supported by an extensive information management network that Bell Canada is building for the 2010 Olympics.

Recently announced improvements to the E-Comm system may indicate what those technological gaps may be. According to media reports, the E-Comm centre is working in conjunction with telecommunications providers to

develop the capability to pinpoint the location of 911 calls made from mobile phones. The concern that is prompting this upgrade is that the large numbers of Olympics tourists unfamiliar with their surroundings, particularly US visitors who are accustomed to emergency systems that have such locational capabilities, may result in many more calls from individuals unaware of their location and, as a consequence, the poor deployment of emergency services (Robertson 2009).

In this regard, Vancouver represents the leading edge of the wider use of mobile phone locational technologies. The Canadian Radio-Television and Telecommunications Commission (CRTC) has recently announced that all mobile phone providers will be required to enable mobile phone locational capabilities for 911 use across Canada by February 2010 (CBC 2009). A new computer-aided dispatch system that will allow for quicker deployment of fire response vehicles has also recently been installed. The system uses GPS devices to show the dispatcher which emergency vehicles are closest to a given location, thus minimizing the amount of time a dispatcher may spend on the radio determining the location of vehicles. GPS units have been installed on 115 fire

trucks across 7 municipalities in the greater Vancouver region (Bellett 2008). Vancouver is also ahead of the national curve when it comes to communications interoperability between emergency response providers. Vancouver-area fire, police, and ambulance responders recently made the switch to a common communications standard (P25) that will allow them to communicate directly with one another, a shift that other jurisdictions in Canada are watching as more agencies conform to that standard (MacLeod 2008).

Federal spending in certain areas of transportation infrastructure security may also be accelerated to meet the Games. Transport Canada recently announced that it will spend \$5.6 million CAN to improve security on BC's ferry system, including the introduction of surveillance cameras, fences and other barriers, training for security guards and new onboard and ship-to-shore communications equipment. Through its *Transit Secure* Program, Transport Canada is also spending over \$7 million CAN for access control measures, communications equipment, a security command centre, security training for personnel, and risk assessments for the Vancouver region's public transit network. Both security efforts are components of

nation-wide spending programs but have been accelerated in Vancouver in time for the Games. The federal Transport minister regards the maritime transportation security program as an 'extra benefit [...] that will be in place in time for the 2010 Olympic Games and Paralympic Games.'

The possibility that CCTV cameras installed specifically for the Olympics will remain in place after the Games are over has been raised a number of times in the Canadian media and by civil rights observers in the Vancouver area. Recent Olympics suggest that this is a distinct possibility; approximately 400 of the 1,500 'temporary' CCTV cameras used during the 2004 Athens Games were retained afterwards over and above the proliferation of cameras implemented elsewhere under the broader rubric of Olympics security at locations such as the new airport, public transportation hubs, and public highways. Our discussion with one security official involved in the 2006 Turin Games confirmed that similar CCTV retention occurred at the conclusion of those Games.

That said, given that many of the venues for the 2010 Games are already constructed, many of the CCTV cameras used for venue security will be retrofitted onto

existing buildings and, hence, are more likely to be removed once the Games are over. Where the numbers of CCTV cameras are more likely to increase on a lasting basis as a result of the Games are in the transportation sectors that are related to federal spending in securing those networks, as noted above, and along the Sea to Sky Corridor.

An additional area where CCTV is likely to expand after the Games is in the Granville Entertainment District in Vancouver. The Vancouver Police Department has been actively exploring the possibility of using CCTV to monitor public space in Vancouver over the past decade. The first concerted attempt at launching a CCTV program was in 1999, an initiative that targeted Vancouver's Downtown Eastside. The initial proposal was to install 16 CCTV cameras in the neighbourhood in order to monitor the drug trade. The project was shelved by the VPD after they encountered vehement community opposition (Haggerty, Huey, & Ericson 2008). The second attempt, launched in 2006, aimed to install cameras along the Granville Entertainment District, a two-block strip of Granville Street between Smithe and Helmcken. Unlike the previous attempt that concentrated on the problem of drug use, this plan accentuated problems related to

disorder and civil unrest. The 1994 Stanley Cup riot and 2002 Guns & Roses riot are frequently singled out as instances where CCTV could have helped to maintain public order. More recently, 'counter terrorism issues' and the upcoming need for 'heightened security around Olympic domain which would be imperative for Olympic security' (VPB 2006: 3) have been cited as reasons to support the use of CCTV in the downtown core. A full business case was due before the Vancouver Police Board in May of 2007 for planned budgetary approval in October 2007 and an implementation of 'Phase One' targeted for early 2008. However, none of these deadlines were met, and it seems that the VPD has dropped this initiative as well, though the reasons for doing so are unknown.

In the same year as this proposal was initially formulated (2006) Vancouver City Hall initiated *Project Civil City*, a wide-ranging major initiative designed to curb disorder in Vancouver by 2010 and after. CCTV is proposed as one component of this initiative to 'deter public disorder and support our police in the capturing of individuals breaking the law' (City of Vancouver 2006c: 11). *Project Civil City* appears to have reanimated the VPD actions on CCTV use as the March 2007 Project Civil City

Progress Update indicates that a VPD CCTV project is currently underway (City of Vancouver 2007: 25-26). The same report indicates that 'there is opposition to this type of program by both the provincial and federal Privacy Commissioners' and that 'works [sic] needs to be done to garner their approval' (City of Vancouver 2007: 25-26). More recently the BC Ministry of Public Safety and Solicitor General and the BC Ministry of Attorney General have announced plans to grant \$1 million (CAN) of initial funds to Vancouver, Surrey and Kelowna to conduct projects measuring the effectiveness of CCTV in monitoring high-crime areas (BC 2008).

While past history suggests that at least some of the CCTV cameras implemented for the Games will remain after they conclude, previous Olympics also indicate that a large component of the technological legacies of the Games come from side projects 'piggybacked' on the Games. These side projects may have more lasting power as their needs are related to long-term issues that, as is commonly claimed, would have required a solution at some point anyways, in contrast to the extraordinary measures related to Olympic-specific needs that are more difficult to rationalize once those extraordinary conditions no

longer exist. In the case of Vancouver some of these side projects include upgrades to the lower mainland's emergency communications centre, federal spending in transportation infrastructure security, and CCTV use in downtown public space.

Beyond the prospect that Olympic surveillance technology will remain in place after the Games, there is the related issue that the Olympics provides an opportunity to introduce and field test surveillance technologies that business logics suggest are ultimately designed to move into wider society after the Games. An example of this occurred at the 2001 Super Bowl in Tampa Bay where, for the first time, security officials deployed a large-scale assemblage of cameras, biometric software and terrorist databases to surreptitiously scan and record the facial image of every spectator at that event. After the Super Bowl the cameras were quickly relocated to a nearby Tampa Bay neighbourhood, where the technology was used to monitor the public streets without the knowledge or consent of local citizens (Gips 2001). This transfer ultimately failed for technological reasons (Stanley & Steinhardt 2002) but it underlines how business and security officials can see major events as a real-world mock-up of security initiatives that can

ultimately be employed in more prosaic situations.

More prominent examples of this dynamic include the counter-terrorist networks being built in New York City and Chicago. New York's *Lower Manhattan Security Initiative* and Chicago's *Virtual Shield* each involve extensive CCTV networks monitored from a central command station and which combine facial recognition software, licence plate detecting cameras, integrated law enforcement databases, and fully interoperable communications networks. While not inspired directly by the Olympics (the *Lower Manhattan Security Initiative* is reportedly inspired by London's 'ring of steel'), both projects rely on IBM's Smart Surveillance System (or S3), a software suite ostensibly capable of detecting abnormal patterns of movement, such as if a person were to remain standing on a subway platform after a number of trains pass by. IBM first developed this software for the 2008 Beijing Games and is now in the process of integrating this system into the New York and Chicago security initiatives (Gardner 2007; McMillan 2008; Shachtman 2008).

In concluding this section on the technological surveillance capacities that are deployed in relation to the Games, it is worth briefly accentuating that the

Olympics are high profile political events that are repeatedly overlaid with national interests and interpreted through a lens of geopolitical animosities. The fact that the political interests of other nations extends to, at a minimum, the security of their visiting athletes, citizens and dignitaries, means secret service agents from assorted nations are also keenly attuned to the minutia of how the Games are organized and secured; concerns which extend to the political situation of the host country.

Such an international security focus can translate into different forms of surveillance which more resemble espionage than the types of routine monitoring we have detailed above. Given that such efforts are wrapped in a cloak of national secrecy it is difficult to ascertain the precise scope or nature of such intelligence gathering. The Athens Games did, however, provide at least a glimpse of the types of national security monitoring that the Olympics can prompt.

In February 2006 the Greek government announced that during the 2004 Olympics, and for at least a year subsequent, unknown individuals had tapped the cell phone of Prime Minister Kostas Karamanlis, as well as those of the ministers of foreign

affairs, defence, public order, justice, and approximately 100 other top government, military, and security officials (including the President's wife). While the culprits of this highly sophisticated cell phone tapping have never been caught, it is widely speculated that it was undertaken by American secret service agents concerned about the security dynamics of the

Athens Games (Kiesling 2006; Samatas forthcoming). It would be naïve to believe that above and beyond the increased local monitoring initiated by the Games, that the presence of the Olympics on Canadian soil does not also translate into increased surreptitious scrutiny of Canadian processes, practices and people by an international cohort of secret service agencies.

Legislative and Policy Legacies: Homelessness, Commercial Rights, and Dissent

Above and beyond the surveillance-related organizational and technological dynamics that the Games tend to initiate, they also typically prompt changes to legislative provisions that address other populations. Here we address these in terms of how the

Olympics can culminate in efforts to 'police the poor,' 'police commercial rights,' and 'police dissent.' These issues have repeatedly arisen in hosting the Games and in the context of Vancouver involve a series of surveillance dimensions.

Policing the Poor

Poverty and homelessness sit uneasily with the commercial aspects of the Games, and particularly with the efforts by the City of Vancouver to showcase itself to a global audience. An exhaustive report examining two decades of Olympic host cities concludes that the Olympics are almost always preceded by large-scale 'cleanup' campaigns aimed at sweeping the homeless out of certain parts of the host city (COHRE 2007). For example, numerous 'Quality of Life' ordinances were passed in Georgia the year after Atlanta won the bid for the 1996 Olympics that prohibited people from sleeping in derelict buildings, begging, or walking through parking lots if they did not own a car. In the 12 months

preceding the Games 9,000 arrest citations were issued using these ordinances, almost 4 times more than in previous comparable periods (COHRE 2007: 119).

For the 2000 Sydney Games, New South Wales passed the *Homebush Bay Operations Regulations* in 1999 granting powers to the Olympic Coordination Authority to remove any person from the Olympic grounds, using reasonable force if necessary, if they contravened a list of inappropriate behaviours that were extremely broad and often highly subjective such as 'causing an annoyance or disturbance,' using 'indecent, obscene, insulting, or threatening language,' or behaving in an

‘offensive/indecent manner.’ These regulations remained in effect to 2002 and joined the existing *Darling Harbour Authority Act* of 1984 that prevented loitering, assembly, and unauthorized/unlicensed commercial activity from the small cluster of high-end restaurants, wine bars, theatres, and other entertainment venues that comprise the Darling Harbour district. Critics argued that these laws, along with the New South Wales Police Department’s strategic commitment to zero tolerance policing, were used almost exclusively against the homeless (Lenskyj 2002).

Vancouver has followed a similar legislative pattern in adopting *Project Civil City* (PCC), a wide-ranging major city initiative that aims to reduce street disorder by 2010 (City of Vancouver 2006c). PCC is explicitly about using the Olympics as a ‘catalyst’ to address disorder in the city. Three specific forms of street disorder – aggressive panhandling, the open trade and use of drugs, and homelessness – are targeted for 50% reductions while non-specific reductions for a host of other ‘quality of life’ issues are also sought. Some of the proposed measures to achieve these goals include cracking down on the scavenger economy by removing or locking back alley dumpsters, realigning

existing city services such that a wide range of city employees are expected to serve as the police’s ‘new eyes and ears on the street,’ increasing the lighting in crime-prone parts of the city, encouraging the Vancouver Police Department to enforce B.C.’s *Safe Streets Act*, and, as noted above, exploring the possible use of CCTV in public space. As should be apparent, many of these measures involve new surveillance practices and formalize a surveillance function for city employees.

Perhaps the most contentious component of *Project Civil City* has been the expansion of the Ambassador Program, an initiative of the Downtown Vancouver Business Improvement Association (DVBIA) to put private security guards on the public streets of DVBIA territory. The Ambassadors have no legal standing to enforce criminal law beyond the normal powers of citizen’s arrest. They do, however, enforce property rights and trespass law on behalf of their client, the DVBIA, and collect information on chronic offenders to be shared with the VPD. The program has been expanded to other BIAs in the downtown Vancouver peninsula through contractual arrangements between those BIAs and the DVBIA, who hold a

trademark on the Ambassador name and their distinctive attire.

Until recently the Ambassador program was funded entirely by BIAs but in November 2007 Vancouver City Hall provided close to \$800,000 CAN to expand it in two ways; to have the Ambassadors operate 24 hours a day in the DV BIA and to conduct a pilot program intended to extend the Ambassadors to other BIAs outside of the downtown core. The VPD objected to this support on the grounds that they believe that any public money spent on public safety ought to be allotted to the police, not a private entity. Advocates for the homeless also charged that the project prioritizes security for the few over social justice for the many (Montgomery 2008; Pivot 2008).

Project Civil City is currently teetering on the brink after the Non-Partisan Party, the municipal political party responsible for creating and implementing PCC and which included the mayor, was defeated in the recent municipal election and replaced by councillors who, during the election campaign, declared that they intended to scrap the project. The first casualty appears to be the office of the *Project Civil City Commissioner*, a \$300,000 CAN per year position that the new city councillors plan

to cut in order to free up some much-needed money. City Hall has also cancelled pending contracts worth \$500,000 CAN to expand the Ambassadors beyond the downtown peninsula into 15 other business improvement districts across the city (Howell 2009b; Rolfsen 2009).

Despite its apparent imminent demise, several attributes of *Project Civil City* may live on in other ways. PCC was never intended to be a vehicle for the direct delivery of services but, according to the PCC Commissioner, to 'help those who have direct responsibility for services and programs to do their job more effectively [...] by bridging jurisdictional boundaries, engaging directly and collaboratively with community stakeholders, advocating for new approaches where appropriate, and monitoring progress' (Plant 2007: 2). One policing approach championed by PCC is based on the assumption that urban decay begins with small acts of disorder that, if left unchecked, can escalate, and can ultimately lead to the destruction of neighbourhoods (Wilson & Kelling 1982). The upshot of this approach for authorities is that it justifies policing and regulatory efforts aimed at even the smallest of incivilities, acts that are often performed by an area's most vulnerable populations.

The 2009 Vancouver Police Department (VPD) Business Plan, the document that outlines the department's strategic direction, embraces this philosophy. One of the main goals of the plan is to 'improve liveability by reducing street disorder' by increased application of the province's *Safe Streets Act* and *Trespass Act*. The Plan states that 'members will continue to receive training to use this existing legislation to specifically combat behavior and activities that contribute to urban decay, including aggressive panhandling, squeegeeing, graffiti, public fighting, open-air drug markets, unlicensed street vending, the scavenger economy, and sleeping/camping in city parks and other public spaces' (VPD 2009: 13). From a policing perspective, one of the advantages of attending to such low-level incivilities is that it also provides a surveillance opportunity, as officers can use such encounters as grounds to run an individual's name through police databases to search for outstanding warrants.

The VPD Business Plan also seeks to establish a higher-

profile police presence in the Downtown Eastside by increasing the number of officers assigned to the Beat Enforcement Team (BET). Having such officers generously use bylaw infraction tickets also appears to be part of the strategy in the DTES. The number of tickets issued by the BET has increased to 439 in 2008 from 247 in the previous year. While few of these fines are ever paid, the VPD insists payment is not the ultimate motivation for issuing such tickets. As one officer explained in the media, ticketing is simply a way to 'change behavior – to get people to stop doing certain things' (Howell 2009a). Ticketing is also a mechanism to collect information that can be subsequently used to forbid individuals from accessing specified public locations. Police officers can 'red zone' or ban an individual from designated areas based on repetitive behaviours which are logged each time a ticket is issued to a particular person. So, any Olympics-related push to use such tickets also culminates in there being more citizens on police databases because they have engaged in low-level incivilities.

Policing Commercial Rights

Protecting the commercial interests of Olympic sponsors is a key component of hosting the Olympic Games. Sponsors who pay large sums to the International Olympic Committee seek assurances that their exclusive marketing and distribution rights will be protected from non-licensed 'ambush' marketers who profit from generating an appearance that they are associated with the Games. Protecting this exclusivity begins with Bylaw 51 of the Olympic Charter (IOC 2007) that precludes the expression of commercial publicity¹¹ not expressly authorized by the IOC inside and within the immediate vicinity of Olympic venues.

Critics have singled out such provisions on the grounds that they amount to a form of censorship in the service of commercial interests. It is also the case that any censoring of products or regulations of signage in the context of the Games depends in the first

¹¹ Section 2 of Bylaw 51 of the International Olympic Committee's *Olympic Charter* states: [2] No form of advertising or other publicity shall be allowed in and above the stadia, venues and other competition areas which are considered as part of the Olympic sites. Commercial installations and advertising signs shall not be allowed in the stadia, venues or other sports grounds.

instance on establishing different monitoring regimes to identify such violations. Indeed, in anticipation of any Olympics Games the host city is subjected to a form of IOC commercial scrutiny and cleansing designed to find and eliminate any unlicensed uses of Olympics images or phrases. During the Games this attention to commercial rights can often result in security officials who work at sporting venues scrutinizing citizens in considerable detail for signs of unlicensed products and unwelcome slogans.

The wide regulatory purview of the Olympic marketing provisions has generated numerous accounts of patrons being unable to purchase merchandise because they carry a MasterCard and not a Visa or of people being required to remove hats bearing non-licensed logos. A journalist at the Sydney Games reported how Coca-Cola, a tier one Olympic sponsor, pressured event organizers to preserve their exclusive marketing rights within the Olympic domain, something that resulted in security guards at venue entrances checking for 'knives, weapons, or cans of Pepsi' (Chaudhary 2000). An example from a 2006 FIFA World Cup match in Germany underlines the

lengths to which protecting exclusive marketing rights can go. Match organizers refused to allow individuals wearing an orange pair of lederhosen that had become popular amongst Dutch fans from entering the venue because the clothing carried a non-licensed beer logo. Hundreds of Dutch fans decided to abandon their pants and watch the match in their underwear rather than miss the event entirely (Harding & Cuff 2006).

Canada, like previous host countries, has passed additional legislation to protect sponsorship rights. While existing trademark infringement legislation may sufficiently protect these commercial rights, 'the sheer volume of possible violations, within a short window of time, are presumed to be the justification for the enhanced protection' (Kitching & Pigeon 2007: 8). Bill C-47, *The Olympic and Paralympic Marks Act*, passed by the federal government in 2007, provides this enhanced protection. Schedule One specifies general words, phrases, and symbols common to all Olympics Games (such as 'Faster, Higher, Stronger' and 'Olympia') that are restricted, while Schedule Two and Three specify those unique to 2010 (Such as 'Vancouver, 2010,' and '21st'). The Schedule One restrictions will remain

indefinitely (apparently with an eye to the possibility of future Games in Canada) while the schedule two and three restrictions will expire at the end of 2010.

Businesses using any of the restricted phrases under trademark or license prior to March 2nd 2007 are exempted from the legislation, provided their use is consistent with previous use (Kitching & Pigeon 2007). This exception may have been prompted by the case of *Olympia Pizza*, a family-owned business in Vancouver that was pressured by the IOC and VANOC to change its name and remove its signage before 2010. Bill C-47 allows the restaurant to keep its name but also allows VANOC to press the restaurant to stop displaying the Olympics' 5-ring symbol. It is unclear how VANOC will proceed in this particular instance as they may wish to avoid the widespread public condemnation garnered by their initial attempt to censor the pizzeria. The City of Vancouver has also requested additional powers from the province to regulate signage and other displays on public or private property during the Games. While the city already has some legislative ability to do so, the new powers would allow authorities to act more quickly than current regulations allow and possibly without notifying

the property owner (Montgomery 2009).

Critics argue that while these provisions aim to protect exclusivity rights there is potential for them to be used to stifle free speech (IOCC 2007). Bylaw 51 of the Olympic Charter is written largely in terms regarding commercial trademark infringement, but subsection three of Bylaw 51 specifically prohibits political statements and protest.¹² It was in the spirit of this clause that two black American athletes, Tommie Smith and John Carlos, were expelled from further Olympic competition for raising a gloved fist on the medal podium at the 1968 Mexico City Games, a gesture widely interpreted as a statement voicing protest about treatment of black people in the United States. This provision also applies to fans as well; while national flags are permitted, anyone unfurling a 'Free Tibet' flag, for example, would almost certainly be expelled from the event whether they were at the Beijing or Vancouver Games.

While the Olympic Charter does not carry the force of law, it does slip into the ambiguous realm of the private policing of quasi-

¹² Subsection 3 of Bylaw 51 of the Olympic Charter states: "No kind of demonstration or political, religious or racial propaganda is permitted in any Olympic sites, venues or other areas.

public space. In those contexts decisions about whether someone is included and excluded are often determined by conformity to the instrumental rules of a private entity, not necessarily by adherence to legal or constitutional norms and standards (Shearing & Stenning 1983; Rigakos & Greener 2000). In such contexts, ticket holders not only pay for the privilege of entering an Olympic venue but also open themselves up to a potentially much higher standard of scrutiny than would be tolerated between private citizens and the state, such as random searches, having to provide extensive personal information, or, as noted, refraining from non-sanctioned attire.

Provisions have been built into Bill C-47 to exempt the use of restricted phrases if they are used for criticism, media reporting, and artistic representations, so long as they are not bought and sold for profit. This is being presented as a safeguard against any attempt to use the law to target dissenting opinions and acts (Kitching & Pigeon 2007). Similar legislation at the 2000 Sydney Games¹³ however was criticised for being used in just that manner; as a tool to crack

¹³ The Olympic Arrangements Act (2000).

down on buskers, political and religious demonstrations, individuals wearing anti-corporate logos, and panhandlers (Lenskyj 2002: 59). Direct comparison between Sydney and Vancouver would be misleading as there are, as noted, exceptions contained in Bill C-47 to protect dissenting speech and acts. However, there is still room for abuse if, for example, anti-

Olympic leaflets were (wrongly) removed under the provisions of Bill C-47. That said, the determination of the legality of such exclusions would likely occur long after the Games were over, thus rendering any remedy or penalty largely symbolic as the critical window of opportunity for individuals to communicate their message would have already passed.

Policing Dissent

The Olympics have become a lightning rod for dissent, something that has grown in recent years. The Olympics inevitably attract protestors, some of whom are opposed the Olympics directly and others who seek to use the Games as a platform to publicise other issues. Protests can also sit uneasily with attempts by the host to showcase the city or county, particularly if those protests draw attention to domestic inequalities or if they target visiting heads of state. In this context protests can be particularly embarrassing for the host country.

Managing protest is an integral part of public order policing. This task is magnified at the Olympics because, as noted, the Games often become a focal point for dissent that can unify disparate

movements and draw protestors from afar. While the IOC forbids

the expression of political messages within official Olympic venues, the Olympic Charter does not carry the force of law outside such venues.

In terms of surveillance, the prospect that groups will engage in legal protest at a major event—something that the authorities always fear will culminate in acts violent civil disobedience—has typically motivated security officials such as CSIS to prospectively place organizations and individuals who they see as potentially disruptive under increased covert interpersonal and electronic surveillance. While secrecy protocols mean that we are obviously speculating that this will be the case in Vancouver, the existence and increased use of such scrutiny in

the context of the Olympics would be in keeping with everything that is known about the operation of secret service agencies and is something that many civil libertarians who stand to be subjected to such monitoring believe is already occurring (Garr 2009).

An institutional structure of high-level intelligence and risk assessments has been established to identify such potential threats to the Olympic Games. The Joint Information Group (JIG), an RCMP-lead intelligence group dedicated to the 2010 Olympics consisting of CSIS, the RCMP, and other relevant agencies, is responsible for assessing threats against the Olympics. The JIG interacts with Canada's Integrated Threat Assessment Centre (ITAC), a federal-level intelligence group formed after 9/11 to integrate intelligence and facilitate information sharing within Canada and with its international partners. Representatives from thirteen Canadian agencies staff the ITAC.¹⁴ Intelligence reports

¹⁴ The Canadian agencies represented on the ITAC are Public Safety Canada, Canadian Border Services Agency, Canadian Security Intelligence Service, Communications Security Establishment, Department of National Defence, Foreign Affairs and International Trade Canada, Privy Council Office, Transport Canada, Correctional Service Canada, Financial Transactions and Reports Analysis Centre of Canada, Royal Canadian Mounted Police, Ontario Provincial Police, and Surete du Quebec.

from the JIG and ITAC rate threats against the 2010 Olympics as generally low but have directed surveillance efforts towards a number of specified areas.

There are valid and necessary reasons for these surveillance efforts that we would not dispute. The problem arises when the exceptional character of the Olympics fosters a 'state of exception' mentality wherein more and more citizens are drawn into the widely cast state surveillance apparatus geared towards protecting the Games from terrorism and civil unrest. Terrorism is a famously elastic term that can be defined in widely different ways and has proved to be capable of being advanced as a pretext to monitor a wide range of 'dangerous' or simply unpalatable populations. This was clearly the case in relation to the Beijing Games where the Chinese authorities engaged in intensive surveillance and policing of Tibetan monks, the Uyghur ethnic minority in western China, and revolutionary-prone students whom they deemed a 'terrorist' threat.

Even without the deliberate use of terrorism as a pretext to advance a political agenda, the wide-ranging nature of anti-terrorism legislation post-9/11 can be abused as those powers

devolve into general tools to gather intelligence for investigations that have little or nothing to do with terrorism. Recently released documents obtained from the Maryland State Police Department, for example, show how state troopers had for at least three years invoked anti-terrorism legislation to spy upon Catholic nuns, human rights organizations, church groups, and, in one case, a group advocating for bicycle lanes. Amnesty International was included on this list for the crime of 'human rights.' State police acknowledge that they had used these laws to compile dossiers on 53 individuals, which is an undoubtedly conservative estimate. Interviews with state troopers revealed that many officers did not view the targets of their operations as terrorists but simply used whatever legal tools were available to them to gather as much information as possible about groups in which they had an interest (McDonald 2008). Such practices are in keeping with the general orientation of many police and security organizations to collect masses of information on a 'just in case' basis, storing this data on the grounds that it might prove useful at some point in the future (Ericson & Haggerty 1997).

Such practices can have serious consequences for those caught

up in an anti-terrorism dragnet. Interviews with the Maryland state troopers responsible for their 'anti-terrorism' investigations revealed that they did not contemplate the ramifications of compiling and sharing the names of their 'terrorists' with other government agencies. This was particularly unfortunate as such data sharing effectively cast these 'suspects' into the shadowy realm of government watch lists and perpetual suspicion from which it can be extremely difficult to remove oneself. The assurances of the Maryland troopers that their paper files had been destroyed may be small comfort to those who had inadvertently been investigated using these terrorist provisions, as their names had already been uploaded to federal databases that are routinely recombined, matched with new and old data, and linked in a process of continual analysis. Being mistakenly or carelessly included in these databases can have wide ranging effects for work and personal life. Air travel can be restricted, employment opportunities lost, and families separated forever across political borders. Guilt or innocence may matter little if suspicion is enough to be forever registered on no-fly lists and countless other government databases. As 'need to know' gives way to 'need to share,' such instances are a

reminder of some of the unintended consequences of state surveillance conducted in the name of fighting terrorism.

There are, however, a host of more formal examples of how dissent has been policed in the context of previous Games. The province of New South Wales, for example, passed new legislation to deal with political protests for the 2000 Sydney Games. The *Sydney Harbour Foreshore Authority* of 1999 required all public assemblies taking place on the Sydney harbour area, a complex of parks and open spaces that has traditionally been the starting and/or end point for public rallies and protests in Sydney, to be registered with the Sydney Harbour Foreshore Authority. The Authority was vested with the power to restrict the time, place, and size of any protest or reject or cancel any gathering without notice nor recourse for organizers.

It is notable that these provisions could be applied up to 10 kilometres inland from the waterfront and remained applicable until 2004, which some critics attribute to a political agenda to more aggressively manage annual Australia Day protests by aboriginal groups who dub the holiday 'Invasion Day' and mark it with demonstrations and

marches (Lenskyj 2002: 55-56). This legislation was paired with the NSWs police department's philosophical adherence to a 'zero tolerance' approach to protests that departed from the allowances legislated in the *Foreshore Authority* act. Peter Ryan, Commissioner of the New South Wales Police Department at the time, and lead policing authority for the 2000 Games, expressed this stance prior to the start of the 2000 Games in what can be regarded as a public warning to protestors: 'Australia has always been tolerant of people wanting to express alternative views, politically or otherwise. But we will not tolerate this city being closed down. We will not tolerate any disruption to the Olympic Games. We are not going to have Australia embarrassed' (Chaudhary 2000).


Concerns regarding the possibility of mass protests at the 2000 Games where heightened in part because of the protests that occurred the year before at the World Trade Organization (WTO) summit meetings in Seattle. The WTO protests appeared to announce the arrival of a transnational movement against corporate-driven globalization with which the Olympics seemed to be aligned, if not directly then at least as a vehicle that advances the corporate agenda. The 'Battle

of Seattle' also contributed significantly to a swing towards a paramilitary approach to public order policing featuring highly trained crowd control units, command and control organizational structures, paramilitary dress and equipment, elaborate forms of surveillance, the use of non-lethal weapons, and specialized crowd control techniques. 9/11 furthered this tendency and intensified the state surveillance that protestors were already subject to in the name of fighting terrorism (Warren 2004; Waddington 2008).

Augmenting the police's increasing turn to a paramilitary orientation to regulating dissent has also been an embrace of video cameras. Even at peaceful protests police officials routinely video record protests, and we can anticipate that such recording will occur at any events protesting the Vancouver Olympics. The police see this as a valuable prospective means to gather evidence in case a protest turns violent. Protesters typically see such video recording as a form of intimidation, and they, in turn, sometimes video record police behaviour at demonstrations and picket lines (Hall & de Lint 2003). Police increasingly see the footage they generate as particularly valuable if they want to subsequently identify or arrest unknown

suspects, and towards that end have produced 'video wanted posters,' from these recordings to publicize clips of protests in hopes that a citizen might provide a tip as to the identity of a wanted person. The VPD have a history of using this technique that goes back to their efforts to identify participants in the 1994 Stanley Cup riot (Doyle 2006).

The V2010-ISU has expressed its intention to facilitate the lawful expression of dissent at the 2010 Olympics. A statement released in February 2009 from the V2010-ISU states 'the V2010 Integrated Security Unit and our law enforcement partners within the police forces of jurisdiction will continue to protect the rights of Canadians to voice their opinions using lawful methods and activities, while protecting the public's right to attend the 2010 Olympic and Paralympic Winter Games in peace and safety, without disruption' (V2010-ISU 2009). In the same statement the V2010-ISU rejects speculation that designated protest zones will be used during the Olympics. The image of overzealous police pepper-spraying protestors at the APEC summit at the University of British Columbia in 1997 is not something that the RCMP wants to see repeated (Ericson & Doyle 1999), leading to assurances from the V2010-ISU that 'generous opportunity will be



afforded for peaceful protests to see and be seen in their protest activities by guests to the event.' At the same time the V2010-ISU is prepared to deal resolutely with protests if needed, stating that 'violent or criminal acts that interfere with the rights and

freedoms of law-abiding Canadians and visitors may result in police investigations and criminal prosecutions' and will be 'dealt with quickly,' according to the Chief of the V2010-ISU (Mickleburgh 2009a).

Concluding note

Many organizations now see the Olympics as a stimulus for change. For policing, security and safety officials, the Games present a raft of new challenges, and, as we have demonstrated, surveillance in its many forms has become a central way in which organizations are trying to address those issues.

It should be noted, however, that nothing in this report should be construed to suggest nefarious efforts by Canadian security, safety or law enforcement agencies to install from above a durable legacy of intrusive security and surveillance measure. The introduction of all of these surveillance measures requires no clandestine master builder operating in secret. Instead, the incremental introduction of surveillance measures is undertaken with the best intentions and accelerated by the intense pressures prompted by the Olympics. The expansion of such devices and practises into wider society can typically be explained by the normal operation of a business logic that necessitates that executives try and find new markets for their surveillance products outside of the exceptional circumstances of mega-events.

One of the oft-noted characteristics of the Olympics is their exceptional global visibility. This report should make clear that an unprecedented level of visibility enabled by sophisticated and unprecedented surveillance initiatives is also characteristic of the efforts of host governments to maintain the security of the Olympics. This visibility and concomitant reduction in social privacy produces obvious dangers to civil liberties as Canada and other nations continue their inexorable drift towards a world that is ever more transparent. Each new round of surveillance measures that is introduced simply stands as a temporary launching-off point for the next set of measures which tend to be more penetrating and expansive. There is little to suggest that this process will be measurably slowed at any point in the near future.

Beyond the role that the Olympics play in this overall process of legitimating the introduction and use of surveillance measures, they also play an important but difficult to quantify role in transforming public attitudes towards surveillance. The undeniable physical presence of security

devices and routines at the Games, combined with spectacular representations of such processes by a global media, helps familiarize individuals with the routines of surveillance-infused high security. The Games help attune individuals to new security realities and, in the process, normalizes the routines of personal revelation associated with demands for documents, background checks and expectations that people must reveal themselves and their bodies through assorted screening practices. The proliferating security routines characteristic of mega-events therefore fosters a security-infused pedagogy of acceptable comportment, dress and documentation, as small lessons in security are inflated and played out before a global

audience. This pedagogy in the personal routines of an advanced surveillance infrastructure might be one of the most lasting legacies of mega-events due to how this, in turn, helps fashion a new common sense about surveillance. The undeniable presence of intensive security measures at mega-events reinforces the sense to which it becomes self-evident that such measures are required, that they do not unduly infringe upon personal liberties, that certain dangers are pervasive – and more pressing than other risks – and that the existing constellation of security interests is inevitable. This increasingly normalized spectacle of security can foster a sense in which such assumptions become so self-evident that they are beyond critique.

Glossary

ACOG: Atlanta Committee for the Olympic Games, the organization committee responsible for the 1996 Atlanta Olympic Games.

AWACS: Airborne Early Warning and Control System, an airborne radar system that can dramatically extend the radar and communications capabilities of ground, air, and sea crafts by relaying signals that would otherwise degrade.

BC-IPSU: British Columbia Integrated Public Safety Unit, the unit coordinating provincial emergency and public safety provision for the 2010 Vancouver Olympics.

BET: Beat Enforcement Team, a unit of the VPD deployed in the DTES.

BIA: Business Improvement District, a public-private partnership wherein businesses from a defined geographical zone elect to pay a tax (often based on square footage of occupied space) that is used to fund supplemental projects that enhance that zone and which, it is assumed, translates into boosted economic activity. Street beautification or extra sanitary services are two common examples of such projects.

BTP: British Transport Police.

C4I: Command, Control, Communications, Coordination, and Intelligence, a military alphanumeric acronym meant to underline the concepts integral to total situational awareness. Refers in this report to the surveillance and communications network built by SAIC for the Greek government for the 2004 Athens Olympics.

CBSA: Canadian Border Services Agency.

CCTV: Closed circuit television, the capture and transmission of visual images amongst a limited number of viewing monitors.

CDSS: Command Decision Support System, a major component of the C4I system built for the 2004 Athens Olympics.

CIP: Critical Infrastructure Protection.

COTS: Commercial Off The Shelf, a phrase that refers to any ready-made system that can be 'plugged in' to other systems with only minor adaptations.

CRTC: Canadian Radio-Television and Telecommunications Commission, Canada's federal telecom regulator.

CSIS: Canadian Security and Intelligence Service.

DHS: Department of Homeland Security

DTES: Downtown Eastside, a low-income neighbourhood in downtown Vancouver.

DVBIA: Downtown Vancouver Business Improvement District, Vancouver's largest business improvement district that encompasses much of the city's central business, hospitality and entertainment amenities.

E-Comm: Emergency Communication, in this report referring to the emergency communications center in Vancouver that coordinates emergency services for the lower mainland region of B.C.

EDL: Enhanced drivers' license, a general term for drivers licenses capable of carrying electronic data regarding its carrier.

FBI: Federal Bureau of Investigation.

GIS: Geographic Information System, a term that describes software that stores, organizes,

and displays data that refers or is relevant to a physical location.

GPS: Global Positioning System, a method of determining ground position by triangulating the distance and angles between a ground receiver and a network of satellites.

GSG9: *Grenzschutzgruppe 9* or 'Border Guard Group 9', Germany's elite counter-terrorism unit.

IMSO: Integrated Marine Security Operation, a CAN-US agreement to integrate law enforcement agents from each country onto the coast guard ships of the other country in order to police shared waterways.

INSET: Integrated National Security Enforcement Team. Created in the wake of 9/11 and housed within the RCMP, INSETs are joint counter-terrorism/law enforcement units consisting of the RCMP, CSIS, CBSA, other federal partners, and local law enforcement agencies. INSET units operate in Vancouver, Ottawa, Toronto, and Montreal.

IOC: International Olympic Committee, the international governing body of the Olympic and Paralympic Games.

ITAC: Integrated Threat Assessment Center, Canada's

multi-agency intelligence gathering, integration, and assessment point. ITAC is housed within CSIS.

JIG: Joint Information Group, a multi-agency intelligence group tasked with risk assessment for the 2010 Games. Organizationally, the JIG is a unit of the RCMP.

JTFG: Joint Task Force Games, the code name for Canadian Forces operations for the 2010 Winter Olympics.

MACC: Multi-Agency Communications Center, a general term for any communications center that facilitates the flow of information between public safety, law enforcement, and intelligence agencies. Primarily a US term.

NSSE: National Special Security Event, a US designation for high-profile events with non-routine security needs that, when invoked, defines the organizational roles and responsibilities for federal agencies for the event.

NSW: New South Wales, an Australian province.

OGSD: Olympic Games Security Division, the policing unit within the Greek Ministry of Public Order responsible for security

and public safety planning for the 2004 Athens Olympic Games.

OSSC: Olympic Security Command Centre, the policing unit within the New South Wales Police Force responsible for security and public safety planning for the 2000 Sydney Olympics.

OSD: Olympic Security Directorate, the policing unit within the London Metropolitan Police Service responsible for security and public safety planning for the 2012 London Olympics.

OSSG: Olympic Security Support Group, the policing unit initially responsible for security and public safety planning for the 1996 Atlanta Games. Later replaced by SOLEC.

PCC: Project Civil City, a major city initiative of the City of Vancouver to reduce street disorder by 2010.

PNWER: Pacific North West Economic Region, a public-private partnership devoted to advancing the collective economic interests of British Columbia, Alberta, the Yukon, Alaska, Idaho, Montana, Oregon, and Washington.

RCMP: Royal Canadian Mounted Police, Canada's federal police

RFID: Radio frequency identification, a technology used to identify and track items (inventory, animals, people, etc.) using radio waves. RFID 'tags' containing identifying information of varying amounts can be embedded in an object to be monitored, which can then be identified at a distance by a scanner.

SAIC: Science Applications International Corporation, a US aerospace and defence engineering corporation based in San Diego, California.

SOLEC: State Olympic Law Enforcement Command, the policing unit responsible for security and public safety operations for the 1996 Atlanta Olympics.

SSC: Security and Safety Committee, the policing unit responsible for security and public safety planning for the 2006 Turin Winter Games.

TOPOFF: Top Officials, refers to a series of high-level counter-terrorism preparedness exercises staged by the US.

UOPSC: Utah Olympic Public Safety Command, the organizational unit responsible for security and public safety operations for the 2002 Salt Lake City Winter Olympics.

USSC: United States 2010 Security Committee, a US security and public safety unit formed for the 2010 Winter Games.

USSS: United States Secret Service.

V2010-ISU: Vancouver 2010 Integrated Security Unit, the policing unit within the RCMP responsible for security and public safety operations for the 2010 Vancouver Olympic and Parlympic Winter Games.

VANOC: Vancouver Organizing Committee for the Olympic and Paralympic Games.

VPD: Vancouver Police Department.

WTO: World Trade Organization.

References

- Armstrong, J. 2003, Oct. 14. Vancouver homeless problem getting worse. *The Globe and Mail*, pg. A.3.
- Baker, B. 2009, Feb. 23. Security systems: games plan. *The Engineer* (online). Retrieved Feb. 24 2009 from www.theengineer.co.uk
- Ball, K., & Webster, F. (Eds.). 2003. *The Intensification of Surveillance*. London: Pluto.
- BBC. 2008, Mar. 4. CCTV plan to boost 2012 security. *British Broadcasting Corporation* (online). Retrieved May 12th 2008 from www.news.bbc.co.uk
- BC. 2008. *Province announces pilot to monitor high-crime areas*. Victoria: Ministry of Public Safety and Solicitor General and Ministry of the Attorney General.
- Bellavita, C. 2007. Changing homeland security: a strategic logic of special event security. *Homeland Security Affairs*. 3(3): 1-23.
- Bellett, G. 2008, Nov. 27. New dispatch system online. *The Vancouver Sun*, pg. A.13.
- Bennett, C. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, Mass.: MIT.
- Bradsher, K. 2007a, Sept. 11. An opportunity for Wall Street in China's surveillance boom. *The New York Times*, pg. A.1.
- . 2007b, Aug. 12. China enacting high-tech plan to track people. *The New York times*, pg. A.1.
- . 2007c, Dec. 28. China finds American allies for security. *The New York Times* (online). Retrieved Jan. 31 2008 from www.nytimes.com
- . 2008, Jan. 31. Keeping and eye on China's security. *The New York Times*, pg. C.1.

- Buntin, J. 2000a. *Security Preparations for the 1996 Centennial Olympic Games (A)*. Cambridge, MA: John. F. Kennedy School of Government, Harvard University.
- . 2000b. *Security Preparations for the 1996 Centennial Olympic Games (B): Seeking a Structural Fix*. Cambridge, MA: John F. Kennedy School of Government.
- . 2000c. *Security Preparations for the 1996 Centennial Olympic Games (C): The Games Begin*. Cambridge: John F. Kennedy School of Government, Harvard University.
- CBC. 2009. Cellphone suppliers must show 911 callers' location by February 2010. *Canadian Broadcasting Corporation* (online). Retrieved Feb. 4 from www.cbc.ca
- Chaudhary, V. 2000, Sept. 15. Sydney in grip of Olympic security. *The Guardian* (online). Retrieved Oct. 15 2008 from www.guardian.co.uk
- China Rights Forum. 2006. IR 2008 update: security in Beijing in 2008 and beyond. *China Rights Forum*. 2(1): 106-110.
- City of Vancouver. 1998. *Program of Strategic Actions for the Downtown Eastside*. Vancouver: City of Vancouver.
- . 1999. *Downtown Eastside Community Monitoring Report*. Vancouver: Planning Department.
- . 2001. *Downtown Eastside Community Monitoring Report*. Vancouver: Planning Department.
- . 2006a. *2010 Olympic and Paralympic Winter Games Draft Strategic Plan, Version 1*. Vancouver: City of Vancouver Office of Olympic Operations.
- . 2006b. *Downtown Eastside Community Monitoring Report, online*. Vancouver.
- . 2006c. *Project Civil City*. Vancouver: City of Vancouver.
- . 2007. *Project Civil City March '07 Progress Update*. Vancouver: City of Vancouver.

- Clement, A., & Bennett, C. 2008. Enhanced driver's licence or national identity card? *The Toronto Star* (online). Retrieved Jan. 17 2009 from www.thestar.com
- COHRE. 2007. *Fair Play for Housing Rights: Mega-Events, Olympic Games and Housing Rights*. Geneva, Switzerland: The Center on Housing Rights and Evictions.
- Cottrell, R. 2003. The legacy of Munich 1972: terrorism, security and the Olympic Games. In M. de Moragas, C. Kennett & N. Puig (eds.), *The Legacy of the Olympics Games 1984 - 2000* (pg. 309-313). Lausanne: International Olympic Committee.
- Curry, B., & Friesen, J. 2009, Price tag for security \$1-billion, Ottawa confirms. *The Globe and Mail*, pg. A.10.
- Dao, J. 2002, Mar. 20. Internal security is attracting a crowd of arms contractors. *The New York Times*, pg. C.1.
- Decker, S. H., Greene, J. R., Webb, V., Rojek, J., McDevitt, J., Bynum, T., Varano, S., & Manning, P. K. 2005. Safety and security at special events: the case of the Salt Lake City Olympic Games. *Security Journal*. 18(4): 65-74.
- Decker, S. H., Varano, S., & Greene, J. R. 2007. Routine crime in exceptional times: the impact of the 2002 Winter Olympics on citizen demand for police services. *Journal of Criminal Justice*. 35(1): 89-101.
- DHS. 2005, Jun. 27. Security and Prosperity Partnership Fact Sheet. *Department of Homeland Security* (online). Retrieved Feb. 12 2008 from www.spp.gov
- Doyle, A. 2006. An alternative current in surveillance and control: broadcasting surveillance footage of crimes. In K. Haggerty & R. Ericson (eds.), *The New Politics of Surveillance and Visibility* (pg. 199-224). Toronto: University of Toronto Press.
- Ericson, R., & Doyle, A. 1999. Globalization and the policing of protest: the case of APEC 1997. *The British Journal of Sociology*. 50(4): 589-608.
- Ericson, R., & Haggerty, K. 1997. *Policing the Risk Society*. Toronto: University of Toronto Press, and Oxford: Oxford University Press.

- Finnegan, P. 2005, Feb. 28. SAIC builds on systems integration. *Homeland Security Today* (online). Retrieved Dec. 21 2008 from www.hstoday.us
- Floridis, G. 2004. Security for the 2004 Athens Olympic Games. *Medeterranean Quarterly*. 15(2): 1-5.
- GAO. 2005. *Olympic Security: U.S. Support to Athens Games Provides Lessons for Future Olympics (GAO-05-547)*. Washington D.C.: United States Government Accountability Office.
- Gardner, D. 2007, Sept. 27. Chicago taps IBM, Firetide to install 'Operation Virtual Shield' *Information Week* (online). Retrieved Feb. 10 2009 from www.informationweek.com
- Garr, A. 2009, Feb. 23. Olympic security infiltrates society. *The Vancouver Courier*, pg. 10.
- Gips, M. 2001. Face off over facial recognition. *Security Management*. 45(5): 12-13.
- Haggerty, K., & Ericson, R. 2000. The surveillant assemblage. *British Journal of Sociology*. 51(4): 605-622.
- . (Eds.). 2006. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.
- Haggerty, K., Huey, L., & Ericson, R. 2008. The politics of sight/site: locating cameras in Vancouver's public space. *Sociology of Crime, Law and Governance*. 10(1): 35-55.
- Hall, A., & de Lint, W. 2003. Policing labour in Canada. *Policing and Society*. 13(3): 219-234.
- Harding, L., & Cuff, A. 2006, Jun. 19. The new World Cup rule: take off your trousers, they're offending our sponsor. *The Guardian* (online). Retrieved Feb. 5 2009 from www.guardian.co.uk
- Health Canada. 1995. Federal Government Responds to the HIV/AIDS Crisis in Vancouver. (online). Retrieved August 09, 2002.
- Hennessy, P., & Leapman, B. 2007, Apr. 2. Ministers plan 'Big Brother' police powers. *The Telegraph* (online). Retrieved Feb. 12 2007 from www.telegraph.co.uk

- Hiller, H. 2006. Post-event outcomes and the post-modern turn: the Olympics and urban transformation. *European Sport Management Quarterly*. 6(4): 317-332.
- Houston Chronicle. 2007, Jan, 25. Olympic security expert: terrorist attack on sports event 'just a matter of time'. *The Houston Chronicle* (online). Retrieved May 13 2008 from www.chron.com
- Howell, M. 2009a, Jan. 28. Cops defend ticketing in the Downtown Eastside. *The Vancouver Courier*, pg. 15.
- . 2009b, Jan. 28. Project Civil City at death's door. *The Vancouver Courier*, pg. 8.
- Huey, L. 2007. *Negotiating Demands: The Politics of Skid Row Policing in Edinburgh, San Francisco, and Vancouver*. Toronto: University of Toronto Press.
- Inwood, D. 2008a, Jul. 22. B.C. pushes to ease 2010 border delays. *The Vancouver Province*, pg. A.13.
- . 2008b, Dec. 14. HD aerial pics aim to bolster 2010 security. *The Vancouver Sun*, pg. A.23.
- IOC. 2007. *Olympic Charter*. Lausanne: International Olympic Committee.
- IOCC. 2007. *Olympic Oversight Interim Report Card: 2010 Olympic Games*. Vancouver: Impact of the Olympics on Community Coalition.
- ITAC. 2008. *2010 Vancouver Winter Olympics: Terrorist Threat to Vancouver Area Facilities*. Ottawa: Integrated Threat Assessment Centre.
- Jane's Intelligence Review. 2007. *Fortress Olympics: Counting the Costs of Major Event Security*.
- Kiesling, J. 2006, Mar. 2. An Olympian scandal. *The Nation* (online). Mar. 20 2008 from www.thenation.com.
- Kitching, A., & Pigeon, M.-A. 2007. *Bill C-47: The Olympics and Paralympic Marks Act*. Ottawa: Library of Parliament Information and Research Service.
- Larson, B. 2008. *2010 Olympics & Paralympics Games Security Committee Update*. Seattle: 2010 Olympic Security Committee.

- Lee, J. 2008a, Jul. 22. 2010 border problems dismissed. *The Vancouver Sun*, pg. B.1.
- . 2008b, City arms latest gear for games security. *The Vancouver Sun*, pg. A.16.
- . 2008c, Jun. 6. VANOC chooses metal detectors against advice. *The Vancouver Sun*, pg. B.5.
- Lees, L. 1998. Urban renaissance and the street: spaces of control and contestation. In N. R. Fyfe (ed.), *Images of the Street: Planning, Identity, and Control in Public Space*. London: Routledge.
- Lenskyj, H. 2002. *The Best Olympics Ever? Social Impacts of Sydney 2000*. Albany: State University of New York Press.
- Lombardo, J., Sniegowski, C., Loschen, W., Westercamp, M., Wade, M., Dearth, S., & Zhang, G. 2008. Public health surveillance for mass gatherings. *John Hopkins Technical Digest*. 27(4): 347-355.
- Lyon, D. 2003. *Surveillance After September 11*. London: Polity.
- . 2004. Globalizing surveillance: comparative and sociological perspectives. *International Sociology*. 19(2): 135-149.
- MacLeod, I. 2008, Dec. 6. Emergency chiefs issue distress call about aging radio systems. *The Ottawa Citizen*, pg. A.1.
- MacPherson, D. 2001. *A Framework for Action: A Four Pillar Approach to Drug Problems in Vancouver*. Vancouver: City of Vancouver.
- Maginer. 2008, Aug. 07. Many eyes will watch visitors. *The Los Angeles Times* (online). Retrieved Oct. 13 2008 from www.latimes.com
- Matas, R. 2001, Dec. 6. Vancouver takes aims at fenced goods. *The Globe and Mail*, pg. A.15.
- Matas, R., & Lehmann, J. 2009, Feb. 14. The money pit. *The Globe and Mail*, pg. F.1.
- McDonald, N. 2008, Jan. 9. Maryland police and their weird war on 'terror'. *The Canadian Broadcasting Corporation* (online). Retrieved Jan. 17 2009 from www.cbc.ca

- McMillan, R. 2008. IBM surveillance will watch over Beijing Olympics. *Network World Canada*. 24(1): 1.
- Merrick, J. 2008, Sept. 28. Security bill for London's 2012 Olympics to hit £1.5 billion - triple the original estimate. *The Independent* (online). Retrieved Oct. 1 2008 from www.independent.co.uk
- Mickleburgh, R. 2008, Nov. 20. Plan to house RCMP on ships sinks. *The Globe and Mail*, pg. A.9.
- . 2009a, Jan. 23. Olympic security boss puts protesters on notice. *The Globe and Mail*, pg. A.5.
- . 2009b, Feb. 12. Olympic security efforts to help curb crime in Canada, IOC leaders says. *The Globe and Mail*, pg. A.9.
- Migdalovitz, C. 2004. *Greece: Threat of Terrorism and Security at the Olympics*. Washington: Congress Research Reports.
- Montgomery, C. 2008, Jan. 15. Police union sues city over use of security guards. *The Province*, Vancouver, pg. A.7.
- Montgomery, C. 2009, Jan. 23. No 'ambush' ads on our streets, city council says. *The Vancouver Province*, pg. A.6.
- Morgan, P. 2007, Planning 2010's protection, part 3: the US Department of Homeland Security looks northward at 2010. *Morgan News* #2653.
- Murphy, B. 2004, Jun 2. Security 'superpower'; Greece's top law enforcement official suggests his country will play a global security role after Athens Olympics. *The Hamilton Spectator*, pg. SP.10.
- O'Connor, A., & Sherman, J. 2008. Biometrics screening for Olympic workers. *The Times* (online). Retrieved May 12 2008 from www.timesonline.co.uk
- Oquirrh Institute. 2002. *The 2002 Olympic Winter Games Security Lessons Applied to Homeland Security*. Salt Lake City: The Oquirrh Institute.
- Oster, S., & Fairclough, G. 2008, Aug. 6. Beijing taxis are rigged for eavesdropping. *The Wall Street Journal*, pg. A.7.

- Paperny, A. 2008, Jul. 23. Speedy border crossings urged for Olympics. *The Globe and Mail*, pg. A.5.
- Park, J. 2005. Governing doping bodies: the world anti-doping agency and the global culture of surveillance. *Cultural Studies*. 5(2): 174-188.
- Perrow, C. 1999. *Normal Accidents: Living with High-Risk Technologies*. Princeton, New Jersey: Princeton University Press.
- . 2008. Complexity, catastrophe, and modularity. *Sociological Inquiry*. 78(2): 162-173.
- Pivot. 2008. *Security Before Justice: A Study of the Impacts of Private Security on Homelessness and Under-Housed Vancouver Residents*. Vancouver: Pivot Legal Society.
- Plant, G. 2007. *Project Civil City Progress Report and Agenda for Action*. Vancouver: Project Civil City Implementation Office.
- PNWER. 2008. *Pacific North West Economic Region Border Charter*. Vancouver, BC: Pacific North West Economic Region.
- PSEPC. 2006. *Security and Prosperity Partnership (SPP) Priority Initiative: Objective 9.2 - Conduct joint training and exercises in emergency response (draft)*. Ottawa: Public Safety and Emergency Preparedness Canada.
- RCMP. 2005. *Financial Resources Gap*. Vancouver: Vancouver 2010 Integrated Security Unit.
- Reese, S. 2008. *National Special Security Events*. Washington D.C.: Congressional Research Service.
- Reeve, S. 2000. *One Day in September*. New York: Arcade Books.
- Rigakos, G., & Greener, D. 2000. Bubbles of governance: private policing and the law in Canada. *Canadian Review of Law and Society*. 15(1): 145-185.
- Robertson, G. 2009, Jan. 12. Games push Vancouver to priority position for 911 upgrade. *The Globe and Mail*, pg. A.1.
- Rolfson, C. 2009, Feb. 6. City vetos additional funding to expand Ambassador program. *The Vancouver Sun*, pg. A.5.

- Ryan, P. 2002. *Keynote Address to the Olympic Security Review Conference*. Salt Lake City: The Oquirrh Institute.
- SAIC. 2008. *SAIC announces acceptance of Greek command, control, communications, coordination, and integration (C4I) system*. San Diego: Science Applications International Corporation.
- Samatas, M. 2004. *Surveillance in Greece: From Anticommunist to Consumer Surveillance*. New York: Athens Printing Company.
- . 2007. Security and surveillance in the Athens 2004 Olympics: some lessons from a troubled story. *International Criminal Justice Review*. 17(3): 220-238.
- . forthcoming. The Greek Olympic phone tapping scandal: a defenceless state and a weak democracy. In K. Haggerty & M. Samatas (eds.), *Democracy and Surveillance*. London: Routledge.
- Shachtman, N. 2008, Apr. 4. NYC is getting a new high-tech defense perimeter. Let's hope it works. *Wired Magazine* (online). Retrieved Feb. 10 2009 from www.wired.com
- Shearing, C., & Stenning, P. 1983. Private security: implications for social control. *Social Problems*. 30(5): 493-506.
- Sherman, J. 2007, Dec. 11. Rising security cost threaten to break the Olympic budget. *The Times* (online). Retrieved May 12 2008 from www.timesonline.co.uk
- SIA. 2007. *China Security Market Report Special Supplement: Olympic Update*. Alexandria, Virginia: Security Industry Association.
- Siemens. 2006. *Siemens succeeds in an Olympian challenge*. Siemens: Siemens Building Technologies Press Release.
- Sinoski, K. 2008, Jun. 18. Getting a handle on the west. *The Vancouver Sun*, pg. B.1.
- Smith, C. 2005, August 11. It's the terror stupid. *The Georgia Straight* (online). Retrieved Jan. 7 2007 from www.straight.com
- Spencer, R. 2008, Jun. 21. Anti-terror force assembled for Olympics. *The Calgary Herald*, pg. A.20.

- Spielman, F. 2009, Feb. 19. Surveillance cams help fight crime, city says. *The Chicago Sun-Times*, pg.
- Stanley, J., & Steinhardt, B. 2002. *Drawing a Blank: The Failure of Facial Recognition Technology in Tampa, Florida*. Washington DC: American Civil Liberties Union.
- Stevens, A. 2007. *Sports Security & Safety: Evolving Strategies for a Changing World*. London: SportBusiness Group.
- Taylor, S. 2008. Kreman to ask feds for Olympics aid. *The Bellingham Herald* (online). Retrieved Jan. 31 2008 from www.bellinghamherald.com
- The National Post. 2006, May 30. Olympic Games give Beijing police a chance to learn car racing. pg. A.13.
- Thompson, D. 2008. Olympic security collaboration. *China Security Review*. 4(2): 46-58.
- Tulloch, J. 2000. Terrorism, 'killing events', and their audience: fear of crime at the 2000 Olympics. In K. Schaffer & S. Sidonie (eds.), *The Olympics at the Millennium: Power, Politics and the Games* (pg. 224-242). New Brunswick, N.J.: Rutgers University Press.
- V2010-ISU. 2009. *Privacy Statement*. Vancouver: Vancouver 2010 Integrated Security Unit.
- van Creveld, M. 1991. *The Transformation of War*. New York: The Free Press.
- VPB. 2006. *Minutes of the May 17 Vancouver Police Board regular meeting*. Vancouver: Vancouver Police Board.
- VPD. 2009. *Vancouver Police Department 2009 Annual Business Plan*. Vancouver: Vancouver Police Department.
- Waddington, D. 2008. *Public Order Policing: Theory and Practice*. Portland, OR: Willan Publishing.
- Walton, G. 2001. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. Montreal: International Centre for Human Rights and Democratic Development.

- Warren, R. 2004. City streets - the war zones of globalization: democracy and military operations on urban terrain in the early twenty-first century. In S. Graham (ed.), *Cities, War and Terrorism* (pg. 214-230). London: Blackwell.
- Whitaker, R. 2006. A Faustian bargain: America and the dream of total information awareness. In K. Haggerty & R. Ericson (eds.), *The New Politics of Surveillance and Visibility* (pg. 141-170). Toronto: University of Toronto Press.
- White, P. 2009, Feb. 18. Unmanned drone prowls over the lonely prairie. *Globe and Mail*, Toronto, pg. A.11.
- Wilson, J. Q., & Kelling, G. 1982. Broken windows. *The Atlantic Monthly*. March(31):
- Wong, E. 2001, Sept. 28. Guard is up for stadium security officials across the country. *The New York Times*, pg. D.8.
- Wong, E., & Bradsher, K. 2008, Aug. 4. As China girds for Olympics, new violence. *The New York Times*, pg. A.1.
- Wood, D., Konvitz, E., & Ball, K. 2003. The constant state of emergency?: surveillance after 9/11. In K. Ball & F. Webster (eds.), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* (pg. 137-150). Sterling, VA: Pluto Press.