6

Policing as Spectacle and the Politics of Surveillance at the Toronto G20

KATE MILBERRY AND ANDREW CLEMENT

This chapter examines publicly prominent features of the security and surveillance assemblage displayed during the G20 Summit in Toronto in June 2010.[1] The main focus is on the surveillance measures deployed by police, particularly as they operated to pre-empt political action, disrupt and criminalize political dissent, and intimidate the public more generally. This security/surveillance spectacle is part of a recent transformation in the policing of protest, which shifted from negotiating the management of protest in collaboration with activists during the 1970s to the current strategy of predictive policing, in which the state and its agents attempt to destabilize social movement mobilization in advance of any actions. We analyze the Toronto G20 case in terms of the ways in which the police used (or not) video surveillance, facial recognition techniques, and Internet monitoring to track, identify, and arrest dissidents, most of whom had the charges against them dropped.

This chapter also examines "citizen surveillance" activities, mainly in the form of digital photographic recordings by individuals shared via social media. Such citizen surveillance played a prominent, but largely unsuccessful, role both in police attempts to identify suspects and in investigations of police wrongdoing.

Finally, we consider the lessons of the G20 weekend in terms of the ambiguously double-edged techno-politics of (in)visibility and identification in an increasingly securitized world.

Introduction

Mega-events such as global economic summits offer opportunities for governments to showcase new securitization measures, including surveillance technologies, and to develop related new techniques for social control. The G20 Summit that took place in Toronto in June 2010 provided just such an opportunity and offers a useful case study for understanding the politics of visibility in a post-9/11 world. In the aftermath of the September 11 terror attacks, the "war on terror," with its pervasive culture of fear, helped accelerate the emerging surveillance society. It also furthered the securitizing agenda of successive American regimes – the tightening of border and airport security, the increasing demand for identification, colour-coded threat schemes, watch lists, no-fly lists, arrests, and deportations. So, too, began a "war on dissent," which targeted intellectuals, social justice activists, and other vocal critics of the status quo, challenging prevailing norms of free speech.[2] Increasing police violence at demonstrations and the political fallout of protest – such as highly publicized arrests, trials, and jail terms – served a critical pedagogical function, putting potentially oppositional publics on notice: to dissent is dangerous.

This chapter examines the role that surveillance – and visual surveillance, in particular – played in the protesting and policing of the Toronto G20. Grounded in a post-9/11 context, we consider several forms of visual surveillance, particularly those deployed by police as they operated to pre-empt political action, criminalize political dissent, and intimidate the public more generally. We examine how law enforcement agencies sought to control public space in order to render citizens more visible and thus more vulnerable to their authority. This was accomplished through pre-emptive securitization and the creation of a security spectacle in advance of the G20 and through a variety of visual surveillance techniques deployed before, during, and after the summit. Increased police aggression toward protesters on the ground was complemented by predictive policing – the "precautionary monitoring through information gathering about organizations."[3]

We analyze the implications of the "asymmetry of visibility" that emerged between police and protesters during the Toronto G20 – an event regarded as one of the most serious breaches of civil liberties in Canadian history. We conclude by considering the lessons to be learned in terms of the ambivalent techno-politics of (in)visibility and identification in an increasingly securitized world.

Mega-protest Policing, the Miami Model, and Securing "Fortress Toronto"

The policing of mega-events has changed markedly in recent years, creating opportunities for new forms of urban securitization and surveillance involving federal policing, intelligence agencies, the military, municipal police, and other government agencies.[4] According to Wood and Abe, mega-events such as major sporting events and political/economic summits "form a crucible of governmental anxieties" that may be temporarily assuaged by highly visible displays of security and surveillance power.[5] In the aftermath of 9/11, public protest took on new contours, eliciting novel responses. Governments and the corporate media invoked the "terrorist threat" to rationalize and normalize a form of security that has since become a key plank of the "war on terror" platform. In many instances, "security" comes most overtly in various forms of surveillance – new ID documentation, intensification of identity checks, installation of video surveillance, screening checkpoints, and the like. Highly touted, these security measures often turn out to be much less effective than claimed, a phenomenon Bruce Schneier terms "security theatre" – a palliative counter-measure intended to provide more the "feeling of security rather than the reality."[6] Marshalling the post-9/11 discourse of fear, the policing of major protests became more aggressive as the United States redefined domestic terrorism to include activists working for peace, social justice, and the environment.[7] This occurred in the midst of an overall shift toward pre-emptive securitization where proportionality – the idea that the level of security measures should be proportional to the risk – appears to have been jettisoned.[8]

"Mega-protests" have characterized the global justice movement since its North American debut at the 1999 massive public demonstrations against the World Trade Organization meetings in Seattle. Mega-protests often occur during mega-events – notably, global economic summits hosted by unelected world governing bodies such as the WTO, the International Monetary Fund, and the G8/G20. They attract thousands of protesters from a range of grassroots, non-governmental and union groups with a range of agendas, including opposition to the economic austerity programs of neoliberal programs. Such protests often involve direct action, including the shutting down of streets and, sometimes, the meetings themselves. The policing of mega-protests differs from traditional policing in a variety of ways, all of which converge under the policing regime known as the Miami Model. An emergent policing regime, the Miami Model

was first identified at the Free Trade Area of the Americas summit held in Miami in 2003. Involving a command-and-control style of policing, the Miami Model is a regime that "relies on high levels of confrontation and force in relation to even minor violations."[9] It is composed of a number of tactics whose central objective is police control of public space. The control of public space relies on mass surveillance, performed via technologies like wireless video camera networks. It also includes more targeted surveillance that renders individual subjects open to police treatment through such techniques as expanded ID checks and arrests, kettling, and other forms of direct surveillance which often draw law-abiding people into criminal justice databases.

Two significant components of the Miami Model are the development of new policing alliances – between the military and police, on the one hand, and between public police and private security, on the other – and the normalization of what Stephen Graham refers to as the "new military urbanism": the transformation of cities into militarized zones.[10] Both of these components have a significant impact on the surveillance practices associated with them.

Described by some as "Fortress Toronto," the host city for the fourth G20 Summit provided an opportunity for the showcasing and honing of mega-protest policing. Toronto was the site of the largest security operation in Canadian history, with an "absolutely massive presence of police and security on the ground."[11] The security apparatus boasted an initial budget of $1 billion, including new video surveillance cameras, ten kilometres of security fencing, and twenty thousand police, military, and private security personnel.[12] This security operation was led by the Integrated Security Unit (ISU), a multi-jurisdictional model originally created for the 2010 Vancouver Winter Olympics. Headed by the Royal Canadian Mounted Police (RCMP), the G20 ISU comprised twenty-six police services, including the Toronto Police Service (TPS) and the Canadian Forces.

The shift in mega-protest policing toward the iterative Miami Model also incorporates public pedagogical elements, such as invoking a "state of exception" and preparing the citizenry to tolerate the suspension of their normal rights. According to Giorgio Agamben, a state of exception refers to the increase of power that governments grant themselves in supposed times of crisis, a concept that has taken on new contours in a post-9/11 world.[13] Creating such a state appears intended to produce "cultural acceptance of new security practices" and "wider legitimation of surveillance," regardless of their social costs or outcomes.[14] This was exhibited at the G20 by dramatic displays of the security apparatus revealed in the weeks and days leading up to the summit. These included militarized training exercises; a simulated hostage taking conducted in

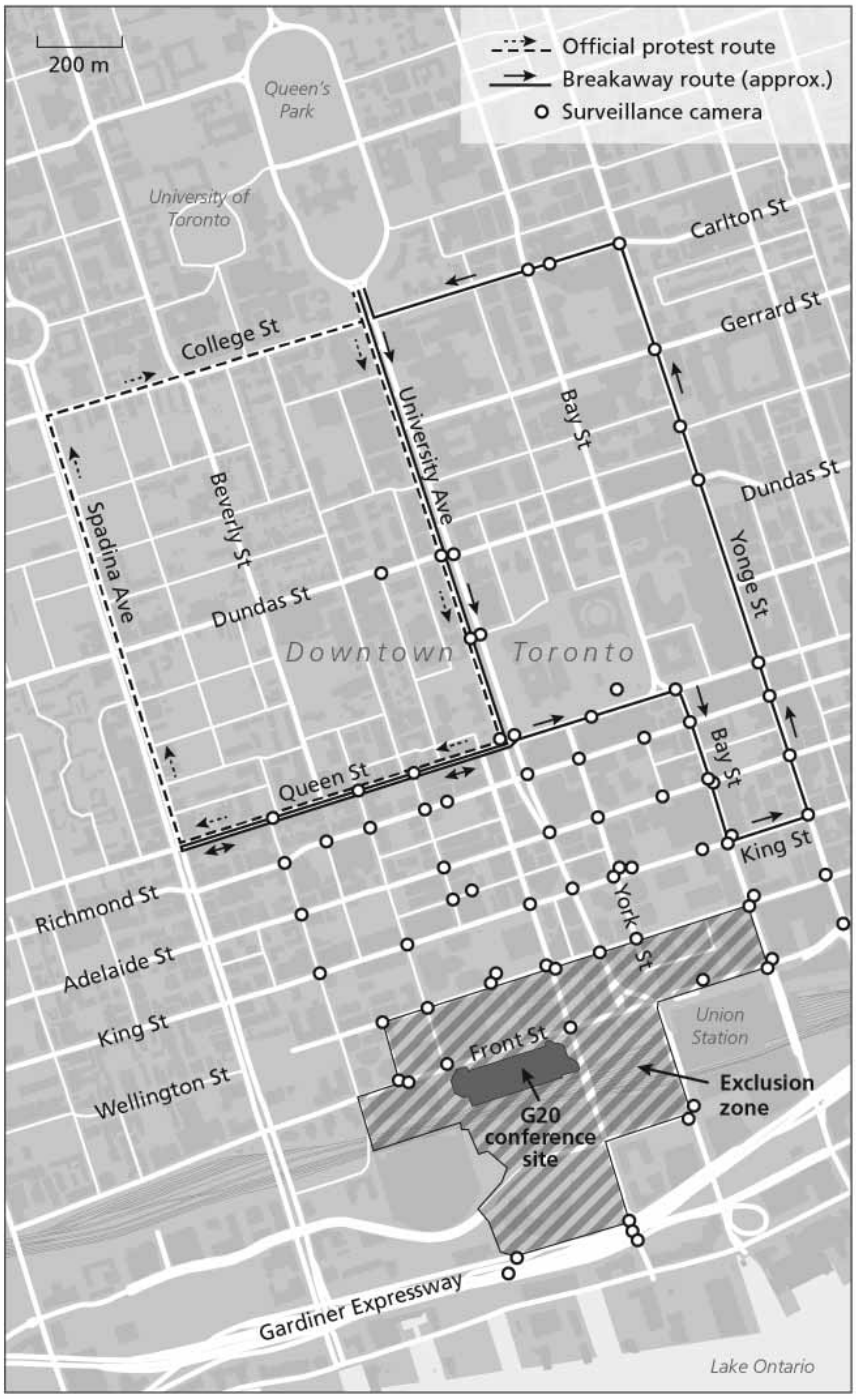
downtown Toronto; the amassing of a large, highly visible police presence on city streets; and "technical briefings." This security spectacle encouraged the gradual normalization of what was otherwise an abnormal situation – the militarization of domestic urban terrain. It also primed the citizen psyche for the violence and exceptionalism associated with militaristic practice, positioning the ensuing police brutality as acceptable.

The Technical Infrastructure of Surveillance: Police Video Cameras

Surveillance, as one of the defining features of the Miami Model, is conducted in a variety of ways during the policing of mega-protests, most obviously by a large, heavily armed, multi-agency police presence. Various surveillance technologies constitute the technical infrastructure of the security spectacle, complementing the work of police on the ground. "A distinctive attribute of securing contemporary mega-events is the increased use of technology," observe Philip Boyle and Kevin Haggerty. This is part of law enforcement's desire to "seamlessly integrate technological, informational and human capabilities in order to hopefully anticipate, detect, and respond to security issues."[15] According to RCMP Chief-Superintendent Alphonse MacNeil, head of G20 security, the ISU's central command centre was capable of monitoring "every aspect of the summit" from its remote location in Barrie, Ontario.[16]

A network of publicly mounted video surveillance cameras constituted a significant part of the G20 security apparatus and was intended to play a strategic role in the control of space for the purposes of surveillance (see Figure 6.1). The Toronto Police Service purchased seventy-one new cameras to add to its seventeen legacy cameras installed in high-traffic entertainment and tourist districts. Initially, the TPS justified the additional G20 cameras as a means "to ensure the safety and security for dignitaries, business owners, residents and people who work and visit the downtown area and protesters."[17] According to signs accompanying the surveillance cameras, their purpose was to "promote public safety and reduce crime." However, the cameras did little to protect citizens during the G20 weekend, during which many law-abiding citizens experienced police brutality, harassment, illegal searches, and mass arrests in full view of the cameras.

Neither did the network of security cameras serve to prevent crime. On the first day of the summit, Saturday, 26 June, a small group of about a hundred (out of thirty thousand) protesters in black clothes and covered faces characteristic of Black Bloc tactics broke from the sanctioned labour march to smash windows of banks, fast-food chains, and other businesses. The surveillance



◄ Toronto Police Service surveillance cameras, installed for the G20.
Source: "G20 Camera Map," *Toronto Star*, http://www.thestar.com/staticcontent/818472.

camera network providing live feeds to the ISU and TPS command centres covered much of the route of this vandalism spree. While police monitored the action, they did not intervene, despite the fact that TPS Chief William Blair was viewing the live feeds from within police headquarters, even as its windows were being smashed.[18] Rather, officers stood down as those involved in the vandalism moved unimpeded through the financial and commercial districts.

In the aftermath of the G20, the function of the video surveillance shifted to forensics, with the cameras upheld as investigative tools that would hold "G20 vandals" to account.[19] Critically, however, the majority of the forty thousand images collected in the hunt for G20 "ringleaders" and others responsible for corporate property damage – 80 percent – came from the public and not from police-owned security cameras.[20] Furthermore, the pictures released as part of the TPS's "most wanted" list appear overwhelmingly to be taken at eye level and not from the height of the pole-mounted video surveillance cameras. Together, these factors cast doubt on the efficacy of the cameras as useful tools for deterring, investigating, or solving such crime.

The public has yet to learn how useful the G20 security cameras were to the TPS's investigation into the property damage. This is because this footage – more than twenty-two thousand hours – has not been released, although Chief Blair pledged to do so.[21] Neither has the TPS released footage from its makeshift jail, which was equipped with "over 100 video cameras that monitored and recorded the movements of prisoners in custody at the facility."[22] Police have denied all but one of the ATI requests for the surveillance footage from the jail where 885 people were detained over the G20 weekend and where human and civil rights abuses were alleged to have occurred.[23] The one picture that was released was too grainy to reprint but sufficiently clear to reveal the squalid and potentially dangerous conditions.

Intelligence Gathering and the Rise of Predictive Policing

Police monitoring and infiltration of activist groups with a potential for protest is a long-standing surveillance tactic. This anticipatory surveillance is a component of predictive policing, a strategy based on intelligence gathering and aimed at pre-empting dissent and subverting social movement mobilizations before they occur.[24] Predictive policing is a hallmark of the Miami Model and is part of an emerging "new penology" that depends "on information, on gauging

probabilities, on a risk calculus and on algorithmic methods and works toward a pre-emptive model for which intensive surveillance is required."[25] The FBI's Counterintelligence Program (COINTELPRO) is a prominent example of how far state agencies will go to monitor, contain, and disrupt legally behaving social movements. Similar, though less well publicized, is PROFUNC (Prominent Functionaries of the Communist Party), Canada's secret plan to identify and intern Communists during the Cold War, which continued until the 1980s.[26]

It appears that the "war on terror" has provided a form of political cover for resuming practices of domestic intelligence gathering of activist groups and disrupting their activities. In Canada, security agencies have recoded "terror identities" from 9/11-style terrorism to ideologically motivated extremisms that encompasses a broad range of grassroots opposition movements such as animal rights, environmentalism, and peace and justice advocacy. This conflation of threat categories has become "a strategy of CSIS to rationalise domestic spying campaigns that target grassroots social movements."[27]

Modes of Police Surveillance

Covert Surveillance

The Toronto G20 repeated this pattern of broad targeting and direct surveillance of social movements, including infiltration, one of the most extreme and disruptive forms of predictive policing. The G20 ISU established a Joint Intelligence Group (JIG) in January 2009 with a mission to conduct "intelligence investigations on possible threats and suspicious activity" surrounding the summit.[28] The "analytical threat picture" developed by JIG was a potpourri of terrorism, environmental activism, "aboriginal/extremist convergence," cyber-espionage, and right-wing extremism. The Primary Intelligence Investigative Team (PIIT) was the investigative arm of JIG responsible for identifying and targeting "suspects, persons of interest and associates in relation to these threats" and for taking steps to "detect, deter, prevent, investigate and/or disrupt threats."[29] The PIIT also compiled a list of suspects, persons of interest, and their associates, names that were redacted in documents acquired through ATI requests.

The PITT adopted a "strategic and global perspective" based on "national and international experiences in a post-9/11 environment."[30] It acquired information using "more covert techniques such as the recruitment of confidential informants and undercover operations."[31] Having determined the possibility of terrorism to be unlikely, the PIIT appears to have focused mainly on the "public

order threat," defined as "criminal extremists motivated by a variety of radical ideologies" like "anarchism, anarcho-syndicalism, nihilism, socialism and/or communism."[32] According to documents obtained through ATI requests, twelve "trained covered investigators" were assigned to "conduct active operations."[33]

As one of the largest domestic intelligence operations in Canadian history, the PIIT "ran undercover operations, recruited confidential informants and liaised with domestic and foreign governments, law enforcement agencies and even corporations."[34] The work of two Ontario Provincial Police officers who infiltrated activist groups in southern Ontario for eighteen months resulted in fifty-nine criminal charges against twenty community organizers alleged to have orchestrated the public disorder during the G20. The court case ended in a plea bargain that saw six of those organizers accept jail time for the crime of "counseling to commit an indictable offence" (a lesser charge than the original one of conspiracy); this case is discussed further in the chapter by Paul Burstein in this volume. The Canadian Civil Liberties Association has called for an investigation into G20 policing, particularly law enforcement's "role in infiltrating protest groups to gather intelligence," noting that "routine infiltration of lawful protest groups" could have "a chilling effect on the rights to freedom of expression and assembly."[35] As one activist noted, "the practice of infiltration and undercover policing of political protest is legally about making a case for conviction, but politically about creating a culture of fear about dissent."[36]

Cyber-surveillance

The intelligence gathering that underpins predictive policing also includes cyber-surveillance, the "monitoring of the internet, cell phones and similar devices ... as a means of pre-empting protest and demonstration."[37] Evidence of specific instances of cyber-surveillance is difficult to muster: this highly technical and largely undetectable form of surveillance is often only confirmed at the outcome of court cases years later or in the rare cases when whistle-blowers have released formerly secret documents. Oliver Leistert's research into cyber-surveillance conducted via the telecommunications infrastructure, for example, was only made possible by released court documents from a seven-year investigation by German authorities of domestic activists.[38] While Deibert et al. document how totalitarian regimes around the world use the Internet to monitor and interfere with human rights activists and political dissidents, Western democracies also engage in government-led spying schemes.[39] The most notorious of these is the "warrantless wiretapping" conducted in the United

States by the National Security Agency (NSA) with the aid of major telecommunications carriers, in effect intercepting the telephone and Internet communications of millions of Americans and other nationals. This first came to public attention in 2006 with revelations by former AT&T technician Mark Klein, but it wasn't until June 2013, with the ongoing publication of whistleblower Edward Snowden's massive trove of leaked NSA documents, that the ominous scope of mass state surveillance became widely known. Stretching the bounds of legality, the Communications Security Establishment Canada (CSEC) facilitated the NSA, its US counterpart, in setting up surveillance facilities within Canada to monitor electronic communications during the G20. Beyond protecting against terrorist attack, according to secret documents reported on by the CBC, the NSA's eavesdropping was aimed at "providing support to policymakers." Indeed, the NSA warned that the more likely security threat would come from "issue-based extremists" conducting acts of vandalism.[40]

Although there is no direct evidence (yet) of the cyber-surveillance of activists mobilizing around the G20, an ATI request revealed that the RCMP established an "internet monitoring unit" with the intention to monitor "all open source internet links related to the G8 G20 summits."[41] The federal government "went to significant lengths to monitor Internet chatter and criticism of the summits ... dissecting, tabulating and reporting on what individuals, unions and universities said on weblogs, Twitter accounts, YouTube and photo sites such as Flickr.com," according to another document obtained through ATI requests.[42] Weekly reports summarized Web commentary to measure public sentiment surrounding various aspects of the G20. One report analyzed 7,250 summit references "to measure how disgruntlement about the security plans for the meetings radiated beyond the mainstream media to non-journalist bloggers."[43] Coupled with anecdotal accounts of email sniffing and other forms of telecommunications monitoring, it seems reasonable to conclude that the ISU engaged in some form of cyber-surveillance as part of its intelligence gathering in the planning and executing of its G20 security plan.

Overt Surveillance

Sometimes intelligence gathering on activists is more visible, apparently intended in part to warn them off action. Another Miami Model tactic, this surveillance takes the rather overt form of physical monitoring – watching activists, calling at their homes, interviewing friends and neighbours, visiting their workplaces, and attending meetings. The Canadian Civil Liberties Association calls it an "intimidating intelligence gathering strategy."[44] Since 9/11, this

type of surveillance has become increasingly commonplace, usually conducted in the immediate lead-up to global economic meetings and experienced by activists as harassment and intimidation.[45] Prior to the Toronto G20, Montreal activist Stefan Christoff said his friends were visited at least five times in the weeks before the summit.[46] Christoff concurs that these types of actions by law enforcement "intend to intimidate and create a political climate of fear within activist networks."[47]

The use of "event monitors" is another form of quasi-overt surveillance used during the G20. According to the RCMP's post-G20 internal report, the goal of the "events monitoring unit" (EMU) was to "monitor crowds and protesters at various demonstrations in Huntsville and Toronto" and "to provide ongoing and real time intelligence by closely monitoring any large gatherings with pre-existing potential for criminality."[48] The EMU teams, composed of TPS and OPP members, "dressed in plainclothes and positioned themselves strategically in order to gather intelligence or evidence in a strictly 'observation' or 'over hear' capacity."[49] Notwithstanding the plainclothes dress of these event monitors, they are often easy to spot, as several YouTube videos make clear, reminding others that they may always be watched.[50]

The overt human surveillance conducted by police was augmented by the technical infrastructure of the G20 surveillant assemblage. In addition to the network of almost one hundred post-mounted video cameras providing live feeds to two command centres, discussed above, law enforcement conducted visual surveillance via police vehicles with internally and externally mounted cameras, as well as various handheld cameras alongside marches and rallies, from behind police lines, and within "kettles." As mentioned, this form of overt surveillance has a dual purpose: to gather intelligence on protesters and to intimidate them. It is an emergent Miami Model tactic that has been contentious in the United Kingdom, where Forward Intelligence Teams (FITs) used photographs taken during protests to create classified "spotter cards." These cards were used by police "to identify individuals they consider to be potential troublemakers because they have appeared at a number of demonstrations," regardless of whether they had criminal records.[51] During the G20, officers routinely filming or otherwise recording law-abiding citizens protesting, observing police actions, or simply passing by seemed to have little other purpose than to gather images for possible later use with facial-recognition technology and/or to send the foreboding message that political assembly and expression are somehow behaviours worthy of police interest. It is not known what police did with those images, how they were stored, or for how long.

Social Media Solicitation and "Crowd-Sourced Surveillance"

A relatively new development in mega-protest policing occurred at the G20, reflecting attempts to more actively integrate the citizenry in the surveillant assemblage. While police have long used "Wanted" posters to enroll citizens in apprehending suspected criminals, the Toronto Police Service took this to a new level in its search for G20 vandals, asking people not only to identify suspects but to submit online images of perpetrators of the property destruction captured on personal cameras and mobile phones. In other words, the TPS invited people to collaborate in their own surveillance by uploading private footage, anonymously, through its website.

From forty thousand images and five hundred videos, mostly submitted by the public, police created "Most Wanted" posters and a social media gallery on Facebook; they then asked people to help identify those engaged in acts they deemed to be illegal. Police called the public response to their appeal "nothing less than remarkable," attributing it to a collective sense of "civic duty."[52] The deputization of citizens en masse to perform unpaid labour for law enforcement is highly problematic, however, for a number of reasons. First, it outsources specialized labour – the gathering of evidence – to untrained individuals with no sworn professional obligations or codes of conduct. Given the formidable difficulties in transforming such images into evidence that can stand up in court, this seems a questionable approach at best. Furthermore, generalized police invitations to report on one's fellow citizens elevates snitch culture to a form of civic responsibility, valorizing a behaviour that Western culture discourages in children: tattling. Alexandra Samuel calls it a form of "crowd-sourced surveillance," and Christopher Parsons points out that it is rife with potential for human rights and civil liberties abuse, including the encouragement of vigilante justice and the human flesh search engine.[53]

Inverse Surveillance: Citizens Look Back

There is a flip side to the growing phenomenon of crowd-sourced surveillance, fuelled by the near ubiquity of personal recording devices: the images captured by citizens can also play a crucial role in calling police to account. Steve Mann calls this phenomenon "inverse surveillance," surveillance that involves "the recording or monitoring of a high ranking official by a person of lower authority."[54] Inverse surveillance is a form of sousveillance, a method of surveillance inquiry that emphasizes "watchful vigilance from underneath."[55] According to the Institute for Applied Autonomy, "inverse surveillance intervenes in the process of surveillance and attempts to undermine or reverse the authoritative

power associated with the technology."[56] Inverse surveillance contributes to "the new visibility in policing" where the technical capacity for surveilling police via the recording and disseminating of images may increase public awareness of police actions as well as police accountability.[57] This is an "explicit strategy of individuals who know very well that mediated visibility can be a weapon in the struggles they wage in their day-to-day lives."[58]

The case of Byron Sonne, a computer security specialist and Toronto resident, offers a dramatic instance of inverse surveillance and the threat with which it is regarded by the state. Concerned by the security theatre surrounding G20 preparations, Sonne joined the Surveillance Club, an informal group of citizens, activists, and academics (including the authors) interested in the "democratic regulation of surveillance technology and practice."[59] There, he announced his intention to perform a "white hat hack" of the G20 security apparatus, with the goal of publicizing apparent weaknesses. White hat hackers specialize in penetration testing to identify and eliminate security flaws. Also referred to as ethical hackers, they breach computer security for non-malicious reasons. As part of his probe, Sonne planned to legally monitor unencrypted police scanners during the G20 and post his findings to Twitter. He also used social media to publish photographs, videos, and tweets documenting and critiquing the securitization of Toronto.

When Sonne hit the G20 security radar, however, it was not due to the extensive surveillance measures, discussed above, that contributed to the G20 security spectacle. Rather, Sonne was discovered quite by accident, after private security informed police about a "suspicious" man photographing the security fence in the days before the summit. A ruse by a Toronto police officer tricked Sonne into providing his identification, which he was not legally required to do.[60] It was this chance encounter that ensnared Sonne in the G20 surveillance net that quickly closed in around him. A subsequent security check by police revealed that he had a firearms licence. Further "open source" investigation by the TPS turned up Sonne's Twitter and Flickr accounts, where he criticized the G20 security theatre and urban militarization of Toronto, as well as his personal blog, where he detailed various amateur science experiments and his anarchist beliefs. From these and other seemingly innocuous data points, police concocted a threat scenario positing Sonne as a politically motivated hacker planning a terrorist attack on the G20. This triggered an intensive five-day surveillance operation, including physical monitoring of Sonne's house and constant daytime tracking of his movements. The operation ended by police surrounding a city bus that Sonne was on and arresting him on the spot. Sonne spent eleven months in jail before being released to await

trial on house arrest. In May 2012, nearly two years after his arrest, he was found not guilty of all charges.

Sonne's ordeal serves as a cautionary tale to activists, political dissenters, and other oppositional publics critical of state actions. As long-time activist Jaggi Singh, also arrested during the Toronto G20, tweeted after Sonne's trial: "The process is the punishment, not the actual verdict (or sentence)."[61]

The Ambivalence of Inverse Surveillance

Punishment by process characterized much of the G20 policing as it sought to contain inverse surveillance. Indeed, many independent journalists were arrested during their efforts to document police officers harassing activists and onlookers for ID or conducting illegal stops and searches. Video footage and photographs taken by hundreds of onlookers, bloggers, citizen journalists, and independent media makers and posted to the Internet confirmed shocking police brutality, as well as disregard for civil liberties and legal protocol, during the G20. The infamous "Officer Bubbles" incident showed TPS officer Adam Josephs threatening to arrest a protester and charge her with assault for blowing bubbles.[62] Captured on video and uploaded to YouTube, the piece went viral. The incident encapsulated what many saw as the key problems with G20 policing: aggressive and threatening behaviour with little restraint or regard for legally protected civil liberties. Despite the broad media coverage and negative public response, however, Josephs was never disciplined.

Some citizen-gathered footage, posted on the Internet and widely circulated via social networking services, became photographic evidence in cases investigating police violence during the G20, including those of Adam Nobody (his real name) and Dorian Barton. Ontario's Special Investigations Unit (ISU) opened an investigation into Nobody's arrest at Queen's Park, the G20 "free speech zone," after a dramatic video showing police beating Nobody was uploaded to YouTube. Although Nobody suffered a shattered cheekbone and broken nose, the ISU soon closed the case for lack of evidence. This was because Nobody's attackers had removed their name badges and no one in the TPS was willing to identify the offending officers.[63] Only after the *Toronto Star*'s two calls for images of the scene garnered video footage from the public did investigators reopen the case.[64] Six months after the incident, the ISU charged Constable Babak Andalib-Goortani with assault with a weapon.[65] A full year after the G20, the ISU charged another TPS officer, Constable Glenn Weddell, with assault causing bodily harm in the Queen's Park arrest of Dorian Barton. Barton suffered a broken arm, a black eye, swollen limbs, and a bruised back at the hands

of his police attackers. The ISU had earlier closed this case too, citing lack of evidence, but reopened it when a bystander came forward with photographs he had taken of the assault.[66]

But these two incidents of inverse surveillance pale in comparison to the widespread police abuses that remain inadequately addressed, despite their broad documentation and dissemination on YouTube and other social networking sites. The CCLA, in its preliminary report on the event, stated that policing throughout the G20 weekend was "at times, disproportionate, arbitrary and excessive."[67] According to André Marin, Ontario's ombudsman, police actions resulted in the "most massive compromise of civil liberties in Canadian history," and the Office of the Independent Police Review Director reported that 469 formal complaints had been filed against police.[68] Two years after the G20, the provincial police watchdog, the Office of the Independent Police Review Director (OIPRD), released a scathing three hundred-page report concluding that "police officers made unlawful arrests, used excessive force and violated protesters' Charter rights."[69] The OIPRD found that three G20 commanders, members of the TPS, had committed misconduct while another twenty-nine officers faced charges of misconduct. To date, however, there has been no public inquiry into G20 policing by the provincial government, despite multiple calls for one.[70]

As Kent Roach notes in Chapter 3, a public inquiry is unlikely in the current political landscape, with both federal and Ontario governments continuing to take advantage of post-9/11 security rhetoric and apparently shameless about the conduct of the police and intelligence communities during the G20. Although multiple reviews of summit policing were completed, they lacked the power and scope of a federal public inquiry, leading to "accountability gaps" across jurisdictions and sectors. However, even if a full public inquiry can plug such gaps, it may fail to result in meaningful policy change, as in the Maher Arar case, where the federal government failed to implement recommendations.

Discussion and Conclusions

The policing and other components of the 2010 Toronto G20 surveillant assemblage raise many disturbing issues that warrant further systematic investigation. In this chapter, we have only scratched the surface, and we have been limited in having had access, for the most part, only to publicly available materials. However, with our focus on visual surveillance as mediated by the Miami Model, we can offer some insights into the role that (in)visibility played in the policing and highlight some possible new directions in this regard.

Like other global economic summits accompanied by a large media corps, the Toronto G20 was made for spectacle and (selective forms of) high public visibility. Demonstrators certainly came seeking attention, wanting to be seen and heard by the gathered leaders and their publics. The police were also visible and likewise apparently intent on sending messages of their own, engaging in a public pedagogy played out through violence, intimidation, and lawlessness. Well beyond protecting world leaders from any possible harm or attempting to intercept or apprehend those who caused property damage, police clearly went out of their way to target protesters and residents more generally. Whether intended or not, the clear lesson was the criminalization of legally protected civil liberties – freedom of speech, assembly, and association. The blame for what unfolded was encapsulated in the words of one police officer, captured in a CBC documentary on the G20: "You should have stayed at home."[71]

This public pedagogy was conveyed largely visually. Far outnumbering the Black Bloc-type protesters but echoing key features of their appearance (e.g., masked and wearing uniformly dark clothing), the police presented themselves in the streets as a collective dominant mass and were prepared to act lawlessly and violently against anyone in their way. While police did not restrict themselves to the Black Bloc method of attacking only property, they mimicked the Black Bloc tactic of anonymity: significant numbers of police sought to "disappear" within the mass by donning full riot gear and removing their name tags, making individual members effectively indistinguishable and contributing to the impunity of their actions.

Despite these efforts, the G20 surveillant assemblage did not perform well, at least in achieving its stated purposes of prevention and securitization. Of the direct surveillance efforts, the overt surveillance performed by the extensive video surveillance camera network failed in every respect. The cameras did not deter vandalism, which occurred largely within their view. After the fact, the recorded images were apparently of no use in identifying or prosecuting offenders because of their viewing distance and angle. Nor have the recordings yet been made public, so they cannot help with answering important questions about police and protester actions. Likewise, the video footage from the temporary jail, where many of the alleged police abuses took place, has not been made widely available. Once again, those caught in the wide-roaming eye of the G20 surveillant assemblage were rendered vulnerable to the police – in some cases, literally exposed through strip searches – while the police managed to keep specific details of their own activities largely hidden from public view.

The covert surveillance that took place in one of the largest known domestic spying operations in Canadian history was also something of a bust. Despite

having twelve operatives infiltrate activist groups across Canada for eighteen months, the JIG was unable to identify any serious plans for criminal activity besides the highly anticipated "smashy smashy" of the Black Bloc tactic. Nor were the undercover operations able to prevent the one-and-a-half-hour vandalism spree that took place on 26 June, despite foreknowledge of this action. Of the twenty co-accused "ringleaders" of the G20 resistance, only six were convicted in plea agreements, and of lesser offences. Similarly, there is no evidence that cyber-surveillance, if deployed, was of any use to the preventive or investigative roles of police. In the case of Byron Sonne, the G20 surveillant assemblage was an utter failure. It seems the security apparatus was actually as flawed as Sonne suspected, unable to detect what police, and later the state, would present as the summit's gravest threat. It was instead overly suspicious private security guards who tipped off police, triggering an investigation and prosecution based more on fantasy than fact. Where cyber-surveillance, along with the overt and covert surveillance tactics used for the G20, more evidently succeeded is in contributing to the public pedagogy that teaches fear of reprisal for political organizing and public expressions of dissent. This pedagogy helps normalize the eclipsing of law and the curtailment of citizenship that accompany mega-events and, in particular, mega-protests while preparing the citizenry for future states of exception.

A relatively novel feature of the Toronto G20 is the role that crowd-sourced surveillance played. By far the most extensive public visual record of the G20 protests and policing was captured by individuals using their hand-held digital cameras and video recorders and disseminated via social networking sites such as YouTube and Flickr. While this voluminous visual record has helped very little so far in holding either the vandals or the police to account, what comes through more clearly is that it contributes greatly to the overall spectacle. But the effects are ambiguous. On the one hand, there is abundant visual evidence that some people vandalized property, to the point that police and politicians used the well-publicized mayhem as retrospective justification for both the security measures and their high price. On the other hand, there is growing evidence that the police acted illegally and with excessive force. Which of these views ultimately prevails in the political arena is still open, but both the subsequent re-election of a majority federal Conservative government and the rebuff of calls for a broad, independent public enquiry into the G20 suggest that the former view continues to prevail.

Viewed in this light, the Black Bloc tactic of highly visible unidentifiability may turn on itself. While the individuals concerned have largely escaped prosecution, their highly publicized vandalism has predictably overshadowed other

messages and forms of opposition. Indeed, whatever visceral message of rage and resistance against capitalism that may been embodied in the Black Bloc destruction of corporate property is obscured by accusations of criminality and police-orchestrated "manhunts," which distract the public with yet another spectacle. Of greater concern is the way in which police have, in multiple ways, acted above the law even as they are ostensibly upholding it. In particular, while demanding ID from citizens and enrolling them in identifying suspects, they have hidden their own identities and refused to identify wrongdoing within their own ranks. This cannot help but seriously undermine the trust that police need to earn among the public to be effective in their legitimate activities, as well as sharpen differences between those who support the police unquestioningly and those who see the need to hold them to public account.

It remains to be seen whether the Toronto G20 security/surveillance spectacle will be an isolated incident that we will learn to avoid in the future or whether it is a harbinger of future Canadian policing in an increasingly tense, securitized world. At this point, without a deeper public investigation, greater transparency of state actions, and the holding of prominent officials to account, the signs are not good.

Notes

1 This is a revised version of the longer paper presented at the workshop "The Expanding Surveillance Net: Ten Years after 9/11" (http://www.sscqueens.org/survnet_agenda). Correspondence regarding this chapter should be sent to Kate Milberry at kate.milberry@gmail.com.

2 James L. Turk, "Preface," in *Disciplining Dissent: The Curbing of Free Expression in Academia and the Media,* ed. William Bruneau and James L. Turk (Toronto: James Lorimer, 2004), 7-13.

3 Amory Starr, Luis A. Fernandez, and Christian Scholl, *Shutting Down the Streets: Political Violence and Social Control in the Global Era* (New York: New York University Press, 2011), 72.

4 Colin Bennett and Kevin Haggerty, eds., *Security Games: Surveillance and Control at Mega-events* (New York: Routledge, 2011).

5 David Murakami Wood and Kiyoshi Abe, "The Aesthetics of Control: Mega-event and Urban Governance in Japan," in "The City, Sport Mega-events and Security," ed. Richard Giulianotti and Francisco Klauser, special issue, *Urban Studies* 48, 15 (2011): 3241-58.

6 Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (New York: Copernicus Books, 2003), 38.

7 Will Potter, *Green Is the New Red* (San Francisco: City Lights Books, 2011).

8 On the shift toward securitization, see Maureen Webb, *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World* (San Francisco: City Lights Books, 2007); on the jettisoning of proportionality, see Bennett and Haggerty, *Security Games*.

9 Alex S. Vitale, "From Negotiated Management to Command and Control: How the New York Police Department Polices Protests," *Policing and Society* 15, 3 (2005): 283-304.

10 Stephen Graham, *Cities under Siege: The New Military Urbanism* (Brooklyn, NY: Verso Books, 2010).

11 Jennifer Yang, "G-20 Summit Security to Be 'Massive,'" *Toronto Star,* 23 March 2010, http://www.thestar.com/news/gta/torontog20summit/article/784285–g20-summit-security-to-be-massive.
12 Office of the Auditor General, *2011 Spring Report of the Auditor General of Canada,* 2011, http://www.oag-bvg.gc.ca/internet/English/parl_oag_201104_e_35230.html.
13 Giorgio Agamben, *State of Exception* (Chicago: University of Chicago Press, 2005).
14 Bennett and Haggerty, *Security Games,* 12.
15 Philip Boyle and Kevin Haggerty, "Spectacular Security: Mega-events and the Security Complex," *International Political Sociology* 3 (2009): 257-74.
16 "Caper in Charge: Bay Native on Top of Summit Security," *Cape Breton News,* 24 June 2010, http://caperfrasers.wordpress.com/2010/06/25/caper-in-charge/.
17 Mary Vallis, "G20: Security Cameras Installed on Nearly Every Corner of Downtown Toronto," *National Post,* 3 June 2010, http://news.nationalpost.com/2010/06/03/g20-security-cameras-installed-on-nearly-every-corner-of-downtown-toronto/.
18 CBC Fifth Estate, "You Should Have Stayed at Home," documentary, 2011, http://www.cbc.ca/fifth/episodes/2010-2011/you-should-have-stayed-at-home.
19 "The Whole 'Officer Bubbles' Story: Toronto Neighbourhood Responds to G20 Policing," YouTube video, *Real News Network,* 2010, http://www.youtube.com/watch?v=bVwXOKZh4Os.
20 Ian Robertson, "Hunting the Men in Black," *Toronto Sun,* 18 September 2010, http://www.torontosun.com/news/torontoandgta/2010/09/18/15397561.html, and "Hunt for G20 Ringleaders Goes High Tech," *Toronto Sun,* 30 August 2010, http://cnews.canoe.ca/CNEWS/Canada/2010/08/28/15178521.html.
21 "Whole 'Officer Bubbles' Story."
22 TPS, *G20 Summit, Toronto, Ontario, June 2010: Toronto Police Service After-Action Review* (Toronto, ON: Toronto Police Service, June 2011), http://www.torontopolice.on.ca/publications/files/reports/g20_after_action_review.pdf, 44.
23 CCLA, *A Breach of the Peace: A Preliminary Report of Observations during the 2010 G20 Summit,* 29 June 2010, http://ccla.org/wordpress/wp-content/uploads/2010/06/CCLA-G-20-INTERIM-REPORT-A-Breach-of-the-Peace-June-29-2010.pdf.
24 Sasha Costanza-Chock, "The Whole World Is Watching: Online Surveillance of Social Movement Organizations," in *Who Owns the Media? Global Trends and Local Resistance,* ed. Pradip Thomas and Zaharom Nain (London: WACC and Southbound, 2004), 271-92.
25 David Lyon, *Surveillance Studies: An Overview* (Cambridge, UK: Polity Press, 2007), 40.
26 "Secret Cold War Plan Included Mass Detentions," *CBC News,* 14 October 2010, http://www.cbc.ca/news/canada/montreal/story/2010/10/13/profunc-canadian-communist-blacklist.html.
27 Kevin Walby and Jeff Monaghan, "Policing Proliferation: The Militarization of Police and Atomic Energy Canada Limited's Nuclear Response Forces," *Canadian Journal of Criminology and Criminal Justice* 52, 2 (2010): 117-45.
28 ISU JIG, "G8-G20 Summit – ISU JIG Intelligence Report," File Control Number 2009-226305 T54, 3 June 2009, http://www.documentcloud.org/documents/268237-piit-baseline.html#document/p6.
29 Ibid., 9.
30 Rod McCann and Marty Kearns, "G8 Summit ISU Joint Intelligence Group structure and command," 2009, retrieved via access-to-information request, 10, 8.
31 ISU JIG, "G8-G20 Summit."
32 Ibid., 6.
33 Tim Groves, "Living among Us: Activists Speak Out on Police Infiltration," *Biarpatch Magazine,* 1 July 2011, http://briarpatchmagazine.com/articles/view/living-among-us; ISU JIG, "G8-G20 Summit."

34 Tim Groves and Zach Dubinsky. "G20 Case Reveals 'Largest Ever' Police Spy Operation," *CBC News,* 23 November 2011, http://www.cbc.ca/news/canada/toronto/story/2011/11/22/g20-police-operation.html.
35 CCLA, "CCLA Activities in Anticipation of the G8/G20 Summits," 2010, http://ccla.org/our-work/focus-areas/g8-and-g20/ccla-activities-prior-g8-g20/.
36 Groves and Dubinsky, "G20 Case."
37 Lyon, *Surveillance Studies,* 97.
38 Oliver Leistert, "Resistance against Cyber-Surveillance within Social Movements and How Surveillance Adapts," *Surveillance and Society* 9, 4 (2012): 441-56.
39 Ronald J. Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (Cambridge: MIT Press, 2010).
40 James Bamford, *The Shadow Factory: The Ultra-secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008); Mark Klein, *Wiring Up the Big Brother Machine ... and Fighting It* (Charleston, SC: BookSurge, 2009); Steven Levy, "How the NSA Almost Killed the Internet," *Wired,* 7 January 2014, http://www.wired.com/threatlevel/2014/01/how-the-us-almost-killed-the-internet/all/; Greg Weston, Glenn Greenwald, and Ryan Gallagher, "New Snowden Docs Show US Spied during G20 in Toronto," *CBC News,* 7 November 2013, http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448.
41 "ATIP Update: Process Manual," *Paroxysms,* 14 May 2011, https://paroxysms.ca/2011/05/14/atip-update-process-manual/.
42 Steven Chase, "From YouTube to Twitter, Ottawa Heard It All during the G20," *Globe and Mail,* 11 January 2011, http://www.theglobeandmail.com/news/politics/from-youtube-to-twitter-ottawa-heard-it-all-during-the-g20/article1866449/.
43 Ibid.
44 CCLA, Letter to CSIS Director, 7 January 2011.
45 Geordie G. Dent, "Police Visiting Toronto G20 Activists: 'Intimidation' and 'Harassment' Claimed," Toronto Media Co-op, 24 April 2010, http://toronto.mediacoop.ca/story/3286.
46 Stefan Christoff, "Two Activists Speak Out about G8/G20 CSIS Intimidation: Stefan Christoff's Story," *Rabble.ca,* 4 June 2010, http://rabble.ca/news/2010/06/two-activists-speak-out-about-g8g20-csis-intimidation-stefan-christoffs-story.
47 Ibid.
48 RCMP, "Progress: Transformation of the Royal Canadian Mounted Police," 2011, http://www.rcmp-grc.gc.ca/pubs/pro-trans/index-eng.htm, 53.
49 Ibid.
50 *It's the End of the World as We Know It and I Feel Fine,* Bacon Bitz, 23 June 2010, http://submedia.tv/stimulator/2010/06/23/bacon-bitz/.
51 "Spotter Cards: What They Look Like and How They Work," *The Guardian,* 25 October 2009, http://www.guardian.co.uk/uk/2009/oct/25/spotter-cards#.
52 TPS, "Public Outrage Leads to G20 Arrest," n.d., http://www.torontopolice.on.ca/modules.php?op=modload&name=News&file=article&sid=4870.
53 Alexandra Samuel, "After a Loss in Vancouver, Troubling Signals of Citizen Surveillance," *Harvard Business Review,* 16 June 2011, http://blogs.hbr.org/2011/06/in-vancouver-troubling-signals/; Christopher Parsons, "Vancouver's Human Flesh Search Engine," *Technology, Thoughts and Trinkets,* 17 June 2011, http://www.christopher-parsons.com/vancouvers-human-flesh-search-engine/.
54 Steve Mann, "'Sousveillance': Inverse Surveillance in Multimedia Imaging," *Multi-media '04: Proceedings of the 12th Annual ACM International Conference on Multimedia,* 10-16 October 2004, New York, 627.

55 Steve Mann, "Sousveillance, Not Just Surveillance, in Response to Terrorism," *Metal and Flesh* 6, 1 (1 March 2002), http://wearcam.org/metalandflesh.htm.
56 Institute for Applied Autonomy, n.d., http://www.appliedautonomy.com/projects.html#is.
57 Andrew Goldsmith, "Policing's New Visibility," *British Journal of Criminology* 50, 5 (2010): 914-34.
58 John B. Thompson, "The New Visibility," *Theory, Culture and Society* 22, 6 (2005): 31-51.
59 Surveillance Club, surveillanceclub.ca. The website is no longer active but is archived at http://web.archive.org/web/20101210054147/http://surveillanceclub.ca/.
60 Denise Balkissoon, "How Byron Sonne's Obsession with the G20 Security Apparatus Cost Him Everything," *Toronto Life,* May 2011, tp://www.torontolife.com/informer/features/2011/05/03/how-byron-sonne%e2%80%99s-obsessions-with-the-g20-security-apparatus-cost-him-everything/.
61 Tweet from Jaggi Singh, @JaggiMontreal, retrieved from https://twitter.com/JaggiMontreal/status/202423285047246849.
62 "Whole 'Officer Bubbles' Story."
63 Jayme Poisson, "Hearing for Officer Charged in G20 Assault Postponed," *Toronto Star,* 24 January 2011, http://www.thestar.com/news/article/927111–hearing-in-g20-assault-case-postponed.
64 SIU, "Toronto Police Service Police Officer Charged: Case Number: 10-TCI-118," news release, 21 December 2010, http://www.siu.on.ca/en/news_template.php?nrid=802.
65 Rosie DiManno, "Charged G20 Officer Stands Alone," *Toronto Star,* 2 February 2011, http://www.thestar.com/news/article/932537–dimanno-charged-g20-officer-stands-alone.
66 SIU, "Toronto Police Service."
67 CCLA, *Breach of the Peace.*
68 André Marin, *Caught in the Act: Investigation into the Ministry of Community Safety and Correctional Services' Conduct in Relation to Ontario Regulation 233/10 under the Public Works Protection Act* (Toronto: Ombudsman of Ontario, December 2010); OIPRD, "OIPRD Releases Status Update."
69 OIPRD, *Policing the Right to Protest: G20 Systemic Review Report,* May 2012, https://www.oiprd.on.ca/CMS/getattachment/Publications/Reports/G20_Report_Eng.pdf.aspx.
70 Keith Leslie, "McGuinty Rejects Call for Public Inquiry into G20 Secret Law," *Globe and Mail,* 6 May 2011, https://www.theglobeandmail.com/news/national/ontario/mcguinty-rejects-call-for-public-inquiry-into-g20-secret-law/article2013400/.
71 CBC Fifth Estate, "You Should Have Stayed at Home."