CHAPTER II

Forgotten Surveillance: Covert Human Intelligence Sources in Canada in a Post-9/11 World

Steve Hewitt

Introduction

Surveillance does not affect everyone equally. Since Edward Snowden made his initial flight to Hong Kong with a treasure trove of documents digitally stuffed in his computer, stories about the surveillance reach of the modern technological state have abounded and continue to appear on a regular basis. Some accounts focus on generalized surveillance on a global scale; others are of particular interest to certain nations, as in the case of Canada and the Communications Security Establishment (CSE) trial, which involved the interception of Wi-Fi transmissions at a Canadian airport, or, in the United Kingdom, the warrantless interception of the communications of British citizens by Government Communications Headquarters (GCHQ).[1] There is a clear fascination in the media with the technology and the scale of the surveillance and the notion that the risk is equivalent for all of us.

This discourse, however, obscures important points. First, the notion of equality in the face of Big Brother's perpetual gaze in a "panoptic society" is, in several respects, ridiculous. While it is certainly true that all may see their communications intercepted, the key point frequently forgotten in the frenzy of discussion is what happens to the material collected. At this stage, the idea of equality breaks down as notions of threat and deviance emerge.[2] A version of

what sociologist David Lyon refers to as "social sorting" comes into play.[3] Specifically, Lyon argues that

> the key practice here is that of producing coded categories through which persons and groups of persons may be sorted (Cayhan 2005; Lyon 2003b). If personal data can be extracted, combined, and extrapolated in order to create profiles of potential consumers for targeted marketing purposes, then, by a similar logic, such data can be similarly processed in order to identify and isolate groups and persons that may be thought of as potential perpetrators of "terrorist" acts. Such "social sorting" has become a standard way of discriminating between different persons and groups for the purposes of providing differential treatment (whether this is encouraging certain classes of consumer to believe that they are eligible for certain exclusive benefits, for example, through club registration and membership, or facilitating or restricting traffic flow though airports by reference to watch lists and PNR [passenger name record] data).[4]

To put it in more real-world terms, I as a white, Euro-Canadian, middle-class male with slightly left-of-centre political views and agnostic religious beliefs have, through privilege, little to fear from blanket surveillance. Conversely, a change to one or several of those characteristics, such as religious belief, and suddenly a convergence can occur with the characteristics of a marginalized category that has been mapped onto the notion of a "threat" by structures of power. As a result, this shift can lead to far more intrusive surveillance and direct consequences as opposed to simply the collection of data. Accordingly, certain groups and individuals have long been subjected to more intrusive surveillance, and dramatic consequences as a result of that attention, because of their ideology, race, ethnicity, gender, sexuality, religion, nationality, social class, or some combination of these variables.[5] The phenomenon of such targeting is not new, although arguably the scale is.

And although intrusive targeted surveillance can often involve technology, it can also feature a technique that predates the type of observation that is garnering the masses of media coverage in the twenty-first century. It is what Jean-Paul Brodeur referred to as "undercover policing," in that it involves "policing operations which

are covert and involve deception."[6] It is human surveillance carried out by "covert human intelligence sources" or CHIS. A CHIS could be an undercover police officer or intelligence agent, or an informant working on behalf of a state agency.[7] The United Kingdom government offers the following official definition of a CHIS:

> A person is a CHIS if
> a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);
> b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
> c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.[8]

There are significant reasons why CHIS, particularly informants, were crucial for countersubversion investigations in the Cold War and remain critical for counterterrorism investigations in the "War on Terror," including in Canada. In parallel to the famous acronym MICE that explains the motivations of those who spy (Money, Ideology, Compromise/Coercion, Ego/Extortion), these CHIS can be described through the acronym NERD.

N represents the nature of the target. Essentially, the more different the targets are from those tasked with spying on them, the greater the need for the informant version of CHIS. This was true during the Cold War when members of certain Eastern European ethnic groups were targeted because of their involvement in far-left radicalism, and intelligence agencies, whose agents often lacked Slavic language skills, had to recruit numerous informants from within the targeted communities. The lack of diversity within security agencies has also applied to gender in the past. Into the early 1970s, the two main domestic intelligence agencies in Canada and the United States, in part reflecting that policing and intelligence work has been historically gendered male, still did not have female agents or officers. Despite this limitation, they still managed to conduct detailed espionage against women's liberation groups, including all-female gatherings, which could not have occurred without the utilization of informants.[9] This point is even more relevant in today's increasingly multicultural world. Government agencies

are not always diverse enough to have expertise in every language and/or culture. Think of cities like London, New York, and Toronto, which have citizens from every corner of the globe. It is for this reason that the Federal Bureau of Investigation has become increasingly reliant on informants for intelligence-related investigations, more so than for normal criminal work, particularly as a starting point into terrorism investigations.[10] In the United Kingdom, there has been a drive to recruit more informants from among Muslim communities because of the difficulties the police and MI5 have had in penetrating them using their own members, which is in part down to their own failures to reflect the makeup of the communities they are targeting for surveillance.[11]

E stands for ease and effectiveness, which is why CHIS are deployed. In democratic societies, it is often easier to employ informants or deploy undercover agents than to use forms of shadowing involving technology. Both the scandal that erupted in December 2005, when the *New York Times* revealed that the administration of President George W. Bush had been conducting warrantless communications interceptions, and the controversy in relation to Snowden, lack a parallel with CHIS.[12] No similar requirements exist for the deployment of informants or undercover agents.[13] The committee of Senator Frank Church (Church Committee), which in the 1970s investigated wrongdoings by American intelligence agencies, noted this anomaly with respect to informants:

> There is no specific determination made as to whether the substantial intrusion represented by informant coverage is justified by the government's interest in obtaining information. There is nothing that requires that a determination be made of whether less intrusive means will adequately serve the government's interest. There is also no requirement that the decisions of FBI officials to use informants be reviewed by anyone outside the Bureau. In short, intelligence informant coverage has not been subject to the standards which govern the use of other intrusive techniques such as wiretapping or other forms of electronic surveillance.[14]

At the time, the only loosely enforced restrictions on intelligence informants were internal ones included in the FBI's "Manual of Instructions," which it did not publicize, added the Church

Committee.[15] In the 1970s, the McDonald Commission revealed that the Royal Canadian Mounted Police (RCMP) had specific guidelines around keeping control of an informant in terms of avoiding illegal activities that reflected a criminal justice model of policing and not a security and intelligence type of investigation:

> A paid informant may think he has a license to commit any offence in order to feign the desired result. To combat this:
> 1. Do not leave him to his own devices.
> 2. Make him operate on strict instructions.
> 3. At every stage of the operation, set out his limits.
> 4. Tell him that any consideration he may get depends on whether he follows instructions.
> 5. Tell him he has no license to violate the law, but let him use all the stealth and inventiveness he can, provided he stays within the limits you set out for him.[16]

Currently, the Canadian government requires its main intelligence agency, the Canadian Security Intelligence Service (CSIS), to get special political permission, including retroactively, if necessary, when the informant version of a CHIS is utilized against sensitive targets, such as university campuses and churches and mosques, but this use still does not involve the obtaining of a warrant.[17] Since 2000, the *Regulation of Investigatory Powers Act* (RIPA) in the United Kingdom has governed the deployment of informants, including who has authority to authorize their use, but there still is no requirement to obtain a warrant.[18] A CHIS then represents a method of state surveillance that does not require the same legal approvals as does spying through technology. As a Canadian law professor put it in response to a lawsuit brought against a CHIS in 2012 by an activist who had been spied on, "the Supreme Court of Canada has been pretty clear in saying the Charter [of Rights and Freedoms] doesn't protect you from a poor choice of friends. Meaning, if you pick someone to be your friend and it happens to be an undercover cop, that's your problem."[19] A series of court decisions at various levels across Canada support this interpretation.[20] The United States Supreme Court has made similar decisions in the past, in which the court distinguished between types of surveillance. Justice William Brennan articulated the difference this way:

> For there is a qualitative difference between electronic surveillance, whether the agents conceal the devices on their persons or in the walls or under beds, and conventional police stratagems such as eavesdropping and disguise. The latter do not so seriously intrude upon the right of privacy. The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the risk we necessarily assume whenever we speak. But as soon as electronic surveillance comes into play, the risk changes crucially. There is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy.[21]

Then there is the effectiveness that goes with CHIS. This is a particularly useful category for police forces and intelligence agencies, since it allows them to overcome one of the main detriments of technological surveillance: vast quantities of information that cannot be processed in a precise or timely fashion. Informants and undercover state agents represent a precise type of surveillance that in some ways is more difficult, although not impossible, to counteract, as it can come in the form of a friend, colleague, or even family member. Some targets did and do attempt to employ methods to counter informants. Moving to smaller cells with each having little knowledge of the activities of the others is one such method. Questioning members about their backgrounds and political convictions is another. In the 1960s, a countering method might have involved having to partake of drugs as proof of one's counterculture credentials.[22] An additional technique is to require serious criminal activity as a test of the commitment to the group and out of the belief that a CHIS would not engage in such actions. Still, it is a style of information collecting that is active instead of passive, as technological surveillance can be, and brings a precision often missing when technology is deployed.

Nor are the various approaches to surveillance necessarily mutually exclusive. There are ways that surveillance by CHIS can interact with spying via technology, thus increasing both ease and effectiveness. CHIS can use technology to spy on targeted groups or individuals through hidden microphones and cameras, computer spyware, GPS trackers, and other devices. CHIS can also be deployed to investigate online criminal, hacktivist protest, and terrorism cases. A hacker, Adrian Lamo, was responsible in 2010 for revealing to the

US government that Chelsea Manning (formerly Bradley Manning) had leaked classified records to WikiLeaks.[23] A year later, Sigurdur "Siggi" Thordarson supplied information about WikiLeaks and Julian Assange while working as an FBI informant.[24] It emerged via the media in 2012 that a well-known hacker nicknamed Sabu, involved with a hacktivist group known as LulzSec, had been working for several months as an FBI informant.[25]

R represents resources. Professional technological surveillance, in whatever form it takes, is expensive and resource-intensive. Even in the present, basic technological surveillance of a subject, which still on occasion involves physical access to the targeted group or individual's property or body, can involve up to a dozen people performing a variety of tasks.[26] All of these factors make this type of spying by the state in most democratic nations expensive, complicated, and unwieldy, and the incentive to use CHIS that much greater.

Finally, *D* is for destructiveness, which is the impact that the informing and spying have. It is not a coincidence that many of the alternative names applied to CHIS are negative and that those who employ them use neutral or positive terminology such as "source" or "asset."[27] Some of this negativity emanates from the nature of informing and spying, which at its heart involves betrayal, potentially at a fundamental level. But it also relates to the active role that CHIS can take as an agent provocateur, who, far from passively observing events, participates or even takes a lead role in the activities that he or she is spying on. This is the most controversial aspect of all when it comes to this type of spying, as it can lead to allegations of entrapment through manipulation of events by CHIS.[28] It also may become a featured aspect of future Canadian counterterrorism with the Harper government's Bill C-51 and the expanded ability of the CSIS to carry out disruption "measures."[29]

It is this type of human surveillance by CHIS that this chapter is concerned with. The chapter will historicize the emphasis in the domestic security and intelligence field, as opposed to ordinary crime fighting, and explore its use in contemporary Canada, ranging from counterterrorism operations to efforts against political protest. It will also situate the Canadian use within a wider American and British current context that has generated considerable controversy in both countries. Ultimately, the chapter will argue that the same controversy, although frequently muted because those targeted for this type of surveillance are frequently marginalized and thus lack

a media platform or political clout to generate wider attention to their cause, will also emerge in Canada unless more effort is made to regulate and provide external scrutiny of the activities of CHIS. Inevitably, secret activity in which transparency and oversight is lacking or weakened because of the absence of direct supervision, combined with the impact on personal relationships, will lead to abuses and controversy. The catch-22 is that this type of surveillance is frequently effective and deemed necessary, particularly in a counterterrorism context, and thus its use will continue, making the emergence of scandal and controversy a given. In a real sense, then, the concerns raised by the Church Committee in the United States of the 1970s remain relevant to the Snowden era and Canada in the twenty-first century.

> The intelligence informant technique is not a precise instrument. By its very nature, it risks governmental monitoring of Constitutionally-protected activity and the private lives of Americans. Unlike electronic surveillance and wiretaps, there are few standards and no outside review system for the use of intelligence informants. Consequently, the risk of chilling the exercise of First Amendment rights and infringing citizen privacy is increased. In addition, existing guidelines for informant conduct, particularly with respect to their role in violent organizations and FBI use of intelligence informants to obtain the private documents of groups and individuals, need to be clarified and strengthened.[30]

The Canadian Historical Context

The formalized use of CHIS by the Canadian state stretches back into the nineteenth century and the rise of the modern security state. The main target in the 1860s was Irish nationalists, specifically Fenians, who launched five main cross-border attacks, which today would be labelled as terrorism, into both British North America and its successor, the fledgling country of Canada. For British North America, the main security agency was the Western Frontier Constabulary, created, according to a government official, to "find out any attempt to disturb the public peace, the existence of any plot, conspiracy, or organization whereby peace would be endangered, the Queen's Majesty insulted, or her proclamation

of neutrality infringed."[31] Recruited to carry out the work of the new agency were CHIS. By 1870, there were fifty CHIS carrying out undercover work, including several who had infiltrated Irish groups.[32] The Canadian government additionally relied on British intelligence through an informant operating in the United States, although Sir John A. Macdonald remained sceptical regarding the reliability of such individuals: "A man who will engage to do what he offers to do, that is, betray those with whom he acts, is not to be trusted."[33] Later in the early twentieth century, Hindus and Sikhs became the targets of Canadian government CHIS; in turn, several informants were murdered, as was a secret agent who was killed by one of the informants whom he handled.[34]

The extensive and permanent use of CHIS in security and intelligence operations began during the First World War. In echoes of the modern counterterrorism era, the war raised the spectre of an enemy within, particularly in western Canada, which had a large "enemy alien" population drawn from parts of Europe that Canada now warred against. The immediate response on the part of the main security force in the western half of Canada, the Royal North-West Mounted Police (RNWMP), was to recruit informants who had the language and ethnic background that would allow them to move easily among those now under surveillance.[35] Later in the war, police officers from more diverse backgrounds would go undercover as well. The most famous of these was John Leopold, who was originally recruited as an informant but then became a full-time undercover Mounted Policeman because of his "ethnic" appearance and his fluency in Slavic languages. As a CHIS in the 1920s operating under the pseudonym of Jack Esselwein, he infiltrated the fledgling Communist Party of Canada and later became the most famous Mountie in Canada in the interwar period when his real identity was exposed and he testified against his former Communist comrades in an open courtroom.[36]

With the merger of the RNWMP with the Dominion Police, the security force in eastern Canada, the new Royal Canadian Mounted Police appeared in 1920. Its first commissioner, A.B. Perry, helped design the new intelligence agency and put a high priority on CHIS, although he warned that Mountie handlers should "be constantly on their guard against being purposely misled by the informants." One way to do this, he advised, was to have meetings covered by two informants operating independently from each other so that their reports could be compared against each other.[37]

The focus of CHIS for the next several decades when it came to intelligence investigations was almost exclusively on the Communist Party of Canada. This landscape began to change in the 1960s with the emergence of the New Left, Quebec nationalism, Red Power, Black Power, and other movements. The use of CHIS also emerged in the public domain in a controversial fashion that would serve as a preview of the controversy around their use in the post–Cold War, post–9/11 world. In 1961, a student at Laval University was approached by a member of the RCMP and asked to inform on two of her fellow students who were involved in the campus anti-nuclear movement. Instead, she told them about the approach and they went to the media; condemnation of the RCMP effort erupted.[38] This criticism, which the RCMP internally saw as Communist-orchestrated, led to restrictions on the ability of the RCMP to recruit informants on campus, although in practice the impact was negligible.[39] Periodically after the 1960s, controversy around specific CHIS informants would arise. In 1987, it emerged that an informant named Marc-André Boivin had supplied information on the Confederation of National Trade Unions for a number of years to the RCMP and CSIS.[40] In 1992, a journalist revealed that a well-known Quebec provincial cabinet minister in the government of Premier René Lévesque, Claude Morin, had been a paid RCMP informant in the 1970s.[41] Two years later, another journalist broke the story that Grant Bristow, prominent within Canadian far-right circles, had been in the employ of CSIS as an informant for six years.[42] In 2000, the news surfaced that the RCMP had blown up a shed at an oil site to provide credibility to an informant who was attempting to gain the confidence of a farmer who the police believed was engaged in sabotage against the oil industry.[43]

CHIS in Modern Counterterrorism

CHIS have been used and are being used not only in Canada but around the world in the context of domestic security. The post–Cold War security emphasis on counterterrorism has emphasized their significance. While technological surveillance remains important, it is not omnipotent. E-mail can be encrypted and used in different ways, with coded messages hidden within a digitized picture or messages saved in the draft section of an email account and accessed from there instead of being sent out through cyberspace. Rooms can be swept for bugs and terrorists can and do stop using telephones

that are tapped or satellite telephones that reveal their location. Or, if they have to use a telephone, they speak in code with the knowledge that someone somewhere is listening in on the conversation.[44] In 1996, a US Congressional report explicitly addressed the limitations of such surveillance.

> They [technological surveillance methods] do not, however, provide sufficient access to targets such as terrorists or drug dealers who undertake their activities in secret or to the plans and intentions of foreign governments that are deliberately concealed from the outside world. Recruiting human sources — as difficult, imperfect, and risky as it is — often provides the only means of such access.[45]

Former FBI Director Robert Mueller echoes this point

> Human sources…often give us critical intelligence and information we could not obtain in other ways, opening a window into our adversaries' plans and capabilities. [They] can mean the difference between the FBI preventing an act of terrorism or crime, or reacting to an incident after the fact.[46]

Practitioners of counterterrorism have also resorted to CHIS, particularly informants, because of the nature of terrorism. By its core nature, terrorism is an activity of the feeble against the powerful. Weakness often equates with some form of marginalization, be it in terms of language, ethnicity, or religion, or a combination of all of these factors. As a result, as with other intelligence operations in the past, those countering terrorism are not usually drawn from those they are directing attention toward.[47] The increasing problem of Islamist terrorism fits into previous patterns of informant use in the Western world. Intelligence agencies and police services lack the expertise about Muslim communities in general, let alone about small terrorist cells within these groupings. Not surprisingly, then, to gain intelligence police and security agencies frequently have to recruit those on the inside or infiltrate others with a cultural and linguistic familiarity into targeted groups. In the United States, the FBI turned to informants as a solution to its lack of familiarity of Muslim communities. A November 2004 presidential directive required the Bureau to increase "human source" recruitment and control. In

2008, the FBI requested nearly US$13 million to manage its informant system, including through the creation of special software.[48] It was also during this period that the FBI recruited Philip Mudd from the CIA to play a senior role in directing its counterterrorism operations. One of his approaches was "Domain Management," which involved searching for threats within mapped ethnic communities, including through the recruitment of informants.[49]

The FBI's post–9/11 approach to counterterrorism demonstrates a fusion between the uses of informants in intelligence-type operations during the Cold War, such as the targeting of subversion, with the uses of informants in traditional crime fighting. This has led to frequent "sting" operations against alleged terrorists and the heavy involvement of informants in alleged terrorist plots. From 1999 to 2011, of 508 defendants in US terrorism cases, 48 per cent were targeted with informants, 31 per cent were arrested as part of a sting, and 10 per cent were involved in cases where the informant played a lead role in the alleged plot.[50] As will be shown later, this approach has also been used in counterterrorism cases in Canada.

CHIS and Controversy in the United States and the United Kingdom

The use of CHIS in the United States and the United Kingdom has generated different types of controversy and criticism in both countries. In the case of the former, where the CHIS emphasis is on informants, charges of entrapment through agent provocateur activities abound, although they have yet to find any traction with judges or juries in trials. The chief criticism has been that the role of the agent provocateur led to terrorist activities that otherwise would not have occurred. Take the example of Shahed Hussain, a Pakistani immigrant to the United States who arrived in the early 1990s. He eventually became an FBI informant to avoid a jail sentence and in 2004, at the behest of the Bureau, set up a sting in which he offered to sell a missile to two American Muslims for use in an attack on a Pakistani diplomat. Both men were later convicted and sentenced to fifteen years in prison. He then re-emerged in 2008 as an informant in a plot involving four men arrested for trying to blow up a New York City synagogue and shoot down a US military jet. He sold the men a phony bomb and missile, telling one of the men, "Allah didn't bring you here to work for Walmart."[51]

In another instance near Sacramento, California, an informant who received US$250,000 was heard in recordings berating an individual, who was subsequently charged with terrorism offences, for not following through on a promise to attend a terrorism training camp while in Pakistan: "You told me, 'I'm going to a camp. I'll do this, I'll do that.' You're sitting idle. You're wasting time. Be a man — do something!"[52] Then there were the Miami terrorism arrests in 2006, which the administration of President George W. Bush highlighted as the elimination of a serious plot against the United States. Seven men, involved in a bizarre religious group, were charged with various terrorism offences, including plotting to destroy the Sears Tower in Chicago. The Bureau used at least two informants pretending to be al-Qaeda operatives against them; one, who began informing about drug dealers to the New York City Police when he was sixteen, received US$40,000, while the other was paid double that amount. In the end, after two mistrials, a jury convicted five of the accused, although only one on all of the charges.[53]

In the United Kingdom, informants involved in counterterrorism have largely escaped controversy of the type experienced in the United States. A major reason for this is that informants, while still used in counterterrorism cases, do not play a public role in trials as in the American model; hence, their role largely escapes wider public scrutiny. Where controversy has erupted with respect to informants is in relation to their recruitment.[54] More widely in the UK, undercover police officers serving as CHIS in intelligence-led investigations of protest groups have received considerable critical attention. For example, there have been repeated cases of CHIS who had sexual relations with female and male activists they were spying on. In some of these situations, sexual intercourse has been part of a wider long-term relationship between the CHIS and the target. In two cases, the CHIS fathered children with the women they were simultaneously spying on.[55]

Recent Examples of CHIS Use in Canada

Trends in the development of Canada's intelligence agencies and their response to domestic security threats are similar to those in the United States and the United Kingdom. As recounted earlier, during the Cold War, CHIS played a significant role in surveillance against the Communist Party of Canada and then, particularly from the 1960s

onward, against perceived and real threats from both the left and right sides of the political spectrum. That role was primarily led by the Royal Canadian Mounted Police Security Service until 1984 when it was replaced by the Canadian Security Intelligence Service. Even then the RCMP continued to play a role in national security investigations, including counterterrorism, particularly because CSIS does not have the power of arrest. At times, the provincial police forces in Canada's most populous provinces, Ontario and Quebec, would deploy CHIS in intelligence-led investigations.

Indeed, the CHIS activities of the provincial police forces, the Ontario Provincial Police (OPP) and Sûreté du Québec (SQ), have occasionally provoked debate and criticism. In the case of the latter, a well-publicized example of an undercover police officers potentially playing the role of an agent provocateur occurred in 2007 at a summit involving the leaders of Canada, the United States, and Mexico at Montebello, Quebec, when three "demonstrators" dressed as anarchists, including one carrying a rock, were confronted by other protesters. The SQ later admitted that all three men were police officers, although it denied that they were acting as agents provocateurs.[56] In Ontario, in 2010, in the lead up to the meeting of the Group of 20 (G20) conference in Toronto, at least twelve undercover police officers from a variety of forces infiltrated activist groups, including the Steelworkers Organization of Active Retirees and the Toronto Community Mobilization Network, who were preparing to carry out demonstrations. In the case of one Kitchener-Waterloo activist, who subsequently launched a lawsuit against the OPP, the undercover police officer, masquerading as a fellow activist, became a trusted friend, to the point that the CHIS would drive the target's mother to hospital for medical treatments. He later testified against his former protest comrades in a preliminary hearing. Another OPP CHIS moved in and lived with a group of activists in Guelph.[57]

The use of CHIS in post–9/11Canadian counterterrorism cases has also been evident. The most prominent involvement occurred in the so-called Toronto 18 case, in which a group of young Muslim Canadian men sought to carry out terrorist attacks within Canada, including against Prime Minister Stephen Harper. Several informants played a role in the investigation of the case, particularly two in significant roles. The most publicized was Mubin Shaikh, an openly radical Muslim, who provided weapons training to the men. The defence at the trial raised the issue of entrapment, but a judge

subsequently ruled this as irrelevant. Unusually for informants, Shaikh actively courted media attention and would later publish a book about his exploits;[58] he also received nearly C$300,000 for his efforts.[59] It later emerged that a second informant played a more significant role, for which he was paid just under C$4 million along with money for debt repayments and dental work. Shaher Elsohemy, who had previously been an informant for CSIS, agreed to infiltrate the Toronto 18 plotters on behalf of the RCMP in return for a large payment. He originally asked for C$15 million, but a smaller amount was negotiated, although the payment remained controversial. He later testified against the plotters.[60]

Since then, CHIS in the form of both informants and undercover police officers have been involved in two other high-profile Canadian counterterrorism cases that at the time of writing are being tried. One involves two men accused of plotting to carry out an attack on a VIA passenger train travelling from Canada to the United States. That case, a joint American-Canadian investigation, apparently involved an FBI informant, according to American documents.[61] The other case is in British Columbia, where it is alleged that two individuals plotted to carry out a terrorist attack in the vicinity of the BC legislature in Victoria on Canada Day in 2013. The RCMP made it clear that it had used a number of investigative tools and had ensured that the explosive allegedly being constructed by the accused was harmless, prompting speculation that a CHIS had to be involved in a "Mr. Big"-style investigation, in which an undercover police officer poses as a criminal in order to encourage other criminal activity and collect evidence, or an American-style sting involving an informant or informants.[62]

Conclusion: Potential and Future Controversy

Both Canadian history and the use of CHIS in similar countries, specifically the United States and the United Kingdom, show that controversy, criticism, and potential scandal will emerge over the use of CHIS. In some respects, this is inevitable due to the nature of the work. As Julius Wachtel notes, "the individualized nature of police work makes routine oversight inconvenient, if not impossible… [t]he fluid and unpredictable nature of streetlevel encounters gives law enforcment bureaucracies limited leverage over their field personnel."[63] These circumstances are unlikely to change. Indeed, the more

heavily regulated other types of surveillance become in the aftermath of the Snowden revelations, the more the potential there is for CHIS, with fewer restrictions, to be used, particularly in a Canada with a strong emphasis on counterterrorism as a security priority through new legislation. The increased use of CHIS would see a concomitant rise in the potential for controversy and scandal.

On the other hand, the option of not using surveillance by CHIS in counterterrorism cases does not really exist, for the simple reason that such intelligence collection is too valuable and the risk of not preventing potential terrorist attacks too great. CHIS use against non-violent activists is far more problematic and worthy of review because such tactics, in both the past and the present, have the appearance of being undemocratic.

There is, however, a third path, which involves greater transparency and regulation as a means of not eliminating problems but instead reducing or mitigating the circumstances that lead to scandal, controversy, and abuses. Treating human surveillance through CHIS the same as other types of intrusive surveillance, including requiring a warrant before it can be deployed, which was floated in the United States in the 1970s,[64] would be a start along this path.

Notes

1. Greg Weston, Glenn Greenwald, & Ryan Gallagher, "CSEC Used Airport Wi-Fi to Track Canadian Travellers: Edward Snowden Documents," *CBC News*, 30 January 2014, <http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>; Anthony Cuthbertson, "UK Government Admits GCHQ Has Secret Warrantless Surveillance 'Arrangements,'" *International Business Times*, 29 October 2014, <http://www.ibtimes.co.uk/uk-government-admits-gchq-has-secret-warrantless-surveillance-arrangements-1472222>.
2. David Cunningham & Barb Browning, "The Emergence of Worthy Targets: Official Frames and Deviance Narratives within the FBI," (2004) 19:3 *Sociological Forum* 347.
3. David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies," in *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, ed. David Lyon (New York: Routledge, 2005) at 16.
4. David Lyon, "Airport Screening, Surveillance, and Social Sorting: Canadian Responses to 9/11 in Context," (2006) 48:3 *Canadian Journal of Criminology and Criminal Justice* 404.

5. See, for example, William J. Maxwell, *F.B. Eyes: How J. Edgar Hoover's Ghostreaders Framed African American Literature* (Princeton: Princeton University Press, 2015); David J. Garrow, *The FBI and Martin Luther King, Jr.* (New York: Viking, 1983); Christabelle Sethna, "High School Confidential: RCMP Surveillance of Secondary Student Activists," in *Whose National Security? Canadian State Surveillance and the Creation of Enemies*, eds. G. Kinsman, M. Steedman & D. Buse (Toronto: Between the Lines Press, 2000), 121–8; Gary Kinsman & Patrizia Gentile, *The Canadian War on Queers: National Security as Sexual Regulation* (Vancouver: UBC Press, 2010); Ward Churchill & Jim Vander Wall, *Agents of Repression: The FBI's Secret Wars Against the Black Panther Party and the American Indian Movement* (Boston: South End Press, 1988); David Cunnningham, *There's Something Happening Here: The New Left, the Klan, and FBI Counterintelligence* (Berkeley: University of California Press, 2005).
6. Jean-Paul Brodeur, "Undercover Policing in Canada: Wanting What Is Wrong," (1992) 18:1–2 *Crime, Law and Social Change* 105. See generally Gary T. Marx, "Thoughts on a Neglected Category of Social Movement Participant: The Agent Provocateur and the Informant," (1974) 80:2 *American Journal of Sociology* 402; Gary T. Marx, *Under Cover: Police Surveillance in America* (Los Angeles: University of California Press, 1988).
7. See generally Brodeur, *supra* note 6 at 109.
8. UK, United Kingdom Home Office, *Covert Human Intelligence Sources Code of Practice* (London: The Stationery Office, 2010), <www.gov.uk/government/uploads/system/uploads/attachment_data/file/97958/code-practice-human-intel.pdf>.
9. Rush Rosen, *The World Split Open: How the Modern Women's Movement Changed America* (New York: Penguin Books, 2001) at 240–60; Christabelle Sethna & Steve Hewitt, "Clandestine Operations: The Vancouver Women's Caucus, the Abortion Caravan, and the RCMP," (2009) 90:3 *Canadian Historical Review* 463.
10. Lee Romney, "The Trouble with Informants," *Houston Chronicle*, 12 August 2006.
11. Phillip Johnston, "MI5 Seeks 'Older, Wiser Women,'" *Daily Telegraph*, 10 May 2005, <http://www.telegraph.co.uk/news/uknews/1489703/MI5-seeks-older-wiser-women.html>; Michael Evans, "More Britons Are Turning to Terror, Says MI5 Director," *London Times*, 10 November 2006; Barney Calman, "Policing with Passion; Is the Met Police Still Prejudiced against Ethnic Minorities and Women?," *Evening Standard* (London), 10 July 2006.
12. James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, 16 December 2005, <http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0>.

13. See American Civil Liberties Union, "Unnecessary Evil: Blind Trust and Unchecked Abuse in America's Informant System," *American Civil Liberties Union*, <www.aclu.org/unnecessary-evil>.
14. US Government, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans Book III, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Congress* (S Rep No 84-755) (Washington, DC: US Government Printing Office, 1976) at 229–30 [Church Committee Report].
15. *Ibid.*
16. Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Third Report: Certain R.C.M.P. Activities and the Question of Governmental Knowledge* (Ottawa: Supply and Services Canada, 1981) at 317.
17. Steve Hewitt, *Spying 101: The RCMP's Secret Activities at Canadian Universities, 1917–1997* (Toronto: University of Toronto Press, 2002) at 208–11; "Backgrounder No. 1 – The CSIS Mandate," CSIS, February 2005, <http://files.skokos.com/FC-09-3033/Letters-Sent/csis/act/__www.csis-scrs.gc.ca_nwsrm_bckgrndrs_bckgrndr01-eng.pdf>.
18. *Regulation of Investigatory Powers Act* 2000 (UK), c 23; "Covert Human Intelligence Sources," (n.d.), MI5, <https://www.mi5.gov.uk/home/about-us/how-we-operate/gathering-intelligence/covert-human-intelligence-sources.html>. See also Regulation of Investigatory Powers Act 2000 (UK), "Authorisation of Surveillance and Human Intelligence Sources," <http://www.legislation.gov.uk/ukpga/2000/23/part/II/crossheading/authorisation-of-surveillance-and-human-intelligence-sources>.
19. Jennifer Yang, "Activist Sues G20 Undercover Officer Who Was His 'Good Friend,'" *Toronto Star*, 25 April 2012, <http://www.thestar.com/news/gta/2012/04/25/activist_sues_g20_undercover_officer_who_was_his_good_friend.html>.
20. Wendy E. Dawson, *The Use of "Mr. Big" in Undercover Operations*, Course Materials (The Continuing Legal Education Society of British Columbia, 2011) at 5–7; See Edwin W. Kruisbergen, Deborah De Jong & Edward R. Kleemans, "Undercover Policing: Assumptions and Empirical Evidence," (2011) 51:2 *British Journal of Criminology* 394.
21. *Lopez v. United States*, 373 US 427 (1963) at 465, Brennan J., dissenting, cited in Richard C. Donnelly, "Judicial Control of Secret Agents" (1967) 76:5 *Yale Law Journal* 994 at 1009–10.
22. Larry Grathwohl & Frank Reagan, *Bringing Down America: An FBI Informant with the Weathermen* (New Rochelle, NY: Arlington House Publishers, 1976) at 122.
23. Glenn Greenwald, "The Strange and Consequential Case of Bradley Manning, Adrian Lamo and WikiLeaks," *Salon*, 18 June 2010, <http://

www.salon.com/2010/06/18/wikileaks_3/>; Ed Pilkington, "Hacker Who Betrayed Bradley Manning Expresses Regret over Possible Jail Term," *The Guardian*, 15 December 2011, <http://www.theguardian.com/world/2011/dec/15/hacker-adrian-lamo-bradley-manning-wikileaks>.

24. Kevin Poulsen, "WikiLeaks Volunteer Was a Paid Informant for the FBI," *Wired*, 27 June 2013. <http://www.wired.com/2013/06/wikileaks-mole/>.
25. Charles Arthur, Dan Sabbagh & Sandra Laville, "LulzSec Leader Sabu Was Working for Us, Says FBI," *The Guardian*, 7 March 2012, <http://www.theguardian.com/technology/2012/mar/06/lulzsec-sabu-working-for-us-fbi>; Jake Davis, "Sabu, the FBI and Me: How His Light Sentence Affects the Hacking Landscape," *The Guardian*, 28 May 2014, <http://www.theguardian.com/commentisfree/2014/may/28/sabu-fbi-sentence-hackers-anonymous-lulzsec>; Gabriella Coleman, "My Hacker, My Source, My Snitch," *Backchannel*, 10 November 2014, <https://medium.com/backchannel/my-best-hacker-source-was-snitching-for-the-feds-68414d6b552a>.
26. Jeff Sallot, "Canada Could Escape Attack, CSIS Says," *Globe and Mail*, 20 June 2006, <http://circ.jmellon.com/docs/view.asp?id=991>.; Hewitt, *supra* note 17 at 32.
27. Frank J. Donner, *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System* (New York: Vintage Books, 1980) at 464.
28. Trevor Aaronson, "The Informants," 36:5 *Mother Jones* 30, <http://www.motherjones.com/politics/2011/08/fbi-terrorist-informants>.
29. Laura Payton, "C-51 Confusion Abounds As Tories Rush Anti-Terrorism Bill to Committee," *CBC News*, 22 February 2015, <http://www.cbc.ca/news/politics/c-51-confusion-abounds-as-tories-rush-anti-terrorism-bill-to-committee-1.2963569>; "Open Letter to Parliament: Amend C-51 or Kill It," *National Post*, 27 February 2015, <http://news.nationalpost.com/full-comment/open-letter-to-parliament-amend-c-51-or-kill-it>.
30. Church Committee Report, *supra* note 14 at 270.
31. Andrew Parnaby & Gregory S. Kealey, "The Origins of Political Policing in Canada: Class, Law, and the Burden of Empire," (2003) 41:2–3 *Osgoode Hall Law Journal* 211 at 215.
32. *Ibid*.; See also Reg Whitaker, Gregory Kealey & Andrew Parnaby, *Secret Service: Political Policing in Canada from the Fenians to Fortress America* (Toronto: University of Toronto Press, 2012).
33. Parnaby & Kealey, *supra* note 31 at 220–21.
34. *Ibid*. at 237–38.
35. Gregory S. Kealey, "The Early Years of State Surveillance of Labour and the Left in Canada: The Institutional Framework of the Royal Canadian Mounted Police Security and Intelligence Apparatus, 1918–26," (1993) 8:3 *Intelligence and National Security* 129; Steve Hewitt, *Riding to the Rescue:*

The Transformation of the RCMP in Alberta and Saskatchewan, 1914–1939 (Toronto: University of Toronto Press, 2006) at 83–8.

36. Steve Hewitt, "Royal Canadian Mounted Spy: The Secret Life of John Leopold/Jack Esselwein," (2000) 15:1 *Intelligence and National Security* 144.
37. Hewitt, *Riding to the Rescue*, *supra* note 35 at 88.
38. Steve Hewitt, "'Information Believed True': RCMP Security Intelligence Activities on Canadian University Campuses and the Controversy Surrounding Them, 1961–1971," (2000) 81:2 *Canadian Historical Review* 191.
39. *Ibid.*
40. Brodeur, *supra* note 6 at 116.
41. Steve Hewitt, *Snitch!: A History of the Modern Intelligence Informer* (New York: Continuum International Publishing Group, 2010) at 91–2.
42. Andrew Mitrovica, "Front Man," *The Walrus*, September 2004, <http://thewalrus.ca/front-man/>.
43. "RCMP Bombed Oil Site in 'Dirty Tricks' Campaign," *CBC News*, 10 November 2000, <http://www.cbc.ca/news/canada/rcmp-bombed-oil-site-in-dirty-tricks-campaign-1.188599>.
44. Craig Whitlock, "Al Qaeda Detainee's Mysterious Release," *The Washington Post*, 30 January 2006), <http://www.washingtonpost.com/wp-dyn/content/article/2006/01/29/AR2006012901044.html>; Paul Pillar, *Terrorism and U.S. Foreign Policy* (Washington: Brookings Institution Press, 2004) at 112.
45. Mark D. Villaverde, "Structuring the Prosecutor's Duty to Search the Intelligence Community for Brady Material," (2003) 88:5 *Cornell Law Review* 1471 at 1521, citing US, Commission on the Roles and Capabilities of the United States Intelligence Community, 103rd Cong, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Washington, DC: US Government Publishing Office, 1996) at 64, US Government Publishing Office, <www.gpoaccess.gov/int/report.html>.
46. US, Office of the Inspector General, *The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines* (Washington, DC: Office of the Inspector General, Department of Justice, 2005) at 65.
47. Amy Waldman, "Prophetic Justice," *Atlantic Monthly*, October 2006, <http://www.theatlantic.com/magazine/archive/2006/10/prophetic-justice/305234/>; Andrea Elliott, "Undercover Work Deepens Police-Muslim Tensions," *New York Times*, 27 May 2006, <http://www.nytimes.com/2006/05/27/nyregion/27muslim.html?pagewanted=all>;; Dan Eggen, "FBI Agents Still Lacking Arabic Skills," *Washington Post*, 11 October 2006, <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/10/AR2006101001388.html>; See also Pamela Hess, "Intel Agencies Seek Help Recruiting Immigrants," *USA Today*, 17 May 2008, <http://usatoday30.usatoday.com/news/

washington/2008-05-16-intel-recruiting_N.htm>. Steve Hewitt, *The British War on Terror: Terrorism and Counter-Terrorism on the Home Front since 9/11* (London: Continuum, 2008).

48. Aaronson, *supra* note 28.
49. Scott Shane & Lowell Bergman, "F.B.I. Struggling to Reinvent Itself to Fight Terror," *New York Times*, 10 October 2006, <http://www.nytimes.com/2006/10/10/us/10fbi.html?pagewanted=all&_r=0>; Aaronson, *supra* note 28. See also Philip Mudd, *Takedown: Inside the Hunt for Al Qaeda* (Philadelphia: University of Pennsylvania Press, 2013)
50. Aaronson, *supra* note 28.
51. Aaronson, *supra* note 28 (quoting Shahed Hussain); William K. Rashbaum & Kareem Fahim, "Informer's Role in Bombing Plot," *New York Times*, 22 May 2009, <http://www.nytimes.com/2009/05/23/nyregion/23informant.html?pagewanted=all>; Deborah Hastings, "Terrorism Arrests: Snitch, Sting, Then Controversy," *Associated Press*, 24 May 2009; Brendan Lyons, "Mosque Welcomed in Informant," *Albany Times Union*, 8 August 2004. See also Dave Gilson, "FBI Spies and Suspects, in Their Own Words," *Mother Jones*, 10 August 2011, <http://www.motherjones.com/politics/2011/08/fbi-sting-greatest-hits>.
52. Don Thompson, "Tapes: FBI Informant Pushed Suspect into Al-Qaida Camp," *Los Angeles Daily News*, 1 March 2006; Lee Romney, Eric Bailey & Josh Meyer, "Sighting of Terrorist in Lodi Questioned," *Los Angeles Times*, 15 March 2006, <http://articles.latimes.com/2006/mar/15/local/me-lodi15>. See Waldman, *supra* note 47.
53. Mark Hosenball, "Terror Plot Takedown," *Newsweek*, 3 July 2006, <www.newsweek.com>; Bob Norman, "Have Terror, Will Travel," *New Times Broward-Palm Beach*, 22 November 2007, <www.browardpalmbeach.com>; Kirk Semple, "U.S. Falters in Terror Case Against 7 in Miami," *New York Times*, 14 December 2007, <http://www.nytimes.com/2007/12/14/us/nationalspecial3/14liberty.html>; Damien Cave & Carmen Gentile, "Five Convicted in Plot to Blow Up Sears Tower," *New York Times*, 12 May 2009, <http://www.nytimes.com/2009/05/13/us/13miami.html>.
54. Robert Verkaik, "Exclusive: How MI5 Blackmails British Muslims," *The Independent*, 21 May 2009, <http://www.independent.co.uk/news/uk/home-news/exclusive-how-mi5-blackmails-british-muslims-1688618.html>; Vikram Dodd, "Terrorism Act: 'They asked me to keep an eye on the Muslim community,'" *The Guardian*, 23 May 2011, <http://www.theguardian.com/uk/2011/may/23/terrorism-act-muslim>; Aviva Stahl, "Grassing: The Use and Impact of Informants in the 'War on Terror,'" 23:2 *Statewatch* 23, <www.statewatch.org>.
55. Rob Evans & Paul Lewis, "Undercover Police Had Children with Activists," *The Guardian*, 20 January 2012, <http://www.theguardian.com/uk/2012/jan/20/undercover-police-children-activists>. Also see

Paul Lewis & Rob Evans, *Undercover: The True Story of Britain's Secret Police* (London: Faber and Faber, 2013).

56. "Quebec Police Admit They Went Undercover At Montebello Protest," *CBC News*, 23 August 2007, <http://www.cbc.ca/news/canada/quebec-police-admit-they-went-undercover-at-montebello-protest-1.656171>; CanadiansNanaimo, "Police Provocateurs stopped by union leader at anti SPP protest," posted 20 August 2007. https://www.youtube.com/watch?v=St1-WTc1kow.
57. Adrian Morrow & Kim Mackrael, "Publication Ban Lifted on Identities of Undercover G20 Officers," *Globe and Mail*, 22 November 2011, <http://www.theglobeandmail.com/news/toronto/publication-ban-lifted-on-identities-of-undercover-g20-officers/article4184061/; Adrian Morrow & Kim Mackrael, "Undercover Officers Knew of Plans for Downtown Mayhem during G20," *Globe and Mail*, 23 November 2011, <http://www.theglobeandmail.com/news/toronto/undercover-officers-knew-of-plans-for-downtown-mayhem-during-g20/article555130/?page=all>; Tim Groves & Zach Dubinsky, "G20 Case Reveals 'Largest Ever' Police Spy Operation," *CBC News*, 22 November 2012, <http://www.cbc.ca/news/canada/g20-case-reveals-largest-ever-police-spy-operation-1.1054582>; Yang, *supra* note 19.
58. Anne Speckhard & Mubin Shaikh, *Undercover Jihadi: Inside the Toronto 18 – Al Qaeda Inspired, Homegrown Terrorism in the West* (Bassendean, Australia: Advance Press, 2014).
59. Tom Regan, "Is Using Informants in Terror Cases Entrapment?," *Christian Science Monitor*, 13 July 2006; Colin Freeze, "RCMP Agent Concedes Key Role in Set-Up, Running of Terrorist Training Camp," *Globe and Mail*, 31 January 2009; Isabel Teotonio, "No Entrapment, Court Rules in Terror Case," *Toronto Star*, 24 March 2009, <http://www.thestar.com/news/crime/2009/03/24/no_entrapment_court_rules_in_terror_case.html>. See John Miller & Cybele Sack, "The Toronto — 18 Terror Case: Trial by Media? How Newspaper Opinion Framed Canada's Biggest Terrorism Case," (2010) 10:1 *International Journal of Diversity in Organizations, Communities and Nations* 279.
60. Colin Freeze & Omar El Akkad, "Was Imam Another Informant in Toronto Terror Plot?," *Globe and Mail*, 16 January 2007, <www.theglobeandmail.com>; Colin Freeze, "How a Police Agent Cracked a Terror Cell," *Globe and Mail*, 2 September 2009, <www.theglobeandmail.com>; Michael Friscolanti, "Vindication for an Undercover Informant," *Maclean's*, 20 January 2010, <www.macleans.ca>; "Informant's motives Questioned in Toronto 18 Trial,", *CBC News*, 25 January 2010, <www.cbc.ca/news>; Blake Mobley, *Terrorism and Counterintelligence: How Terrorist Groups Elude Detection* (New York: Columbia University Press, 2013) at 218–19.

61. Colin Freeze, "U.S. officials: Train Terror Suspect Suggested Bacteria Plot," *Globe and Mail*, 9 May 2013, <www.theglobeandmail.com>.
62. Steven Chase et al, "RCMP Thwarts Alleged Plot to Bomb B.C. Legislature on Canada Day," *Globe and Mail*, 2 July 2013, <www.theglobeandmail.com>; Bob Mackin, "What Role Did RCMP Play in BC Bomb Plot?," *The Tyee*, 4 July 2013, <thetyee.ca/news>; Bill Tieleman, "Accused's Lawyer Believes Leg Bomb Plot Involved RCMP Sting," *The Tyee*, 13 August 2013, <thetyee.ca>. See generally Dawson, *supra* note 20 for more on "Mr Big" tactics.
63. Julius Wachtel, "From Morals to Practice: Dilemmas of Control in Undercover Policing," (1992) 18 *Crime, Law and Social Change* 137.
64. Federal Bureau of Investigation, *Exhibit 33: Request for Information Concerning This Bureau's Operation of Informants in the Internal Security Field, Church Committee* (Washington, DC: Congress, 1975).

Page left blank intentionally