The Surveillance Legacies of 9/11: Recalling, Reflecting on, and Rethinking Surveillance in the Security Era

David Lyon and
Kevin D. Haggerty

Recalling Security-Era Surveillance

Do we need yet more analysis of the responses to the September 11, 2001 (hereafter 9/11), terrorist attacks? Those tragic events occurred more than a decade ago, and their 10-year memorial focused on bringing "closure" to the event. For many, those attacks have become an increasingly distant, if still poignant, memory. For still others—such as the new cohort of undergraduate students who were only nine years old on the day of the attacks—9/11 is social history.

Our contention in putting together this volume is that there continues to be significant reason to scrutinize 9/11 in terms of its consequences for the dynamics of surveillance. The aftermath of that tragic event played a major role in policy changes and in international relations. Wars were fought in Iraq and Afghanistan, sparked by 9/11, and many thousands more people died as a result. "National security" was elevated to a top priority in the United States and elsewhere, and this approach has had wave and ripple effects throughout the world. This is the "War on Terror," and, unlike other wars, this one has no visible end point.[1] These developments certainly affected surveillance practices internationally and have been the cue for the United States to demand that other countries fall in line with its approach. On the other hand, for many countries, especially in the global south, 9/11 is not a top-of-mind matter, nor is "national security" a vital concern.

The events of 9/11 brought home to ordinary people as never before the fact that we live in what Magnus Hornqvist[2] and others call the "security era." The intensification of surveillance is one key dimension of that security era, which works with the other dimensions to disrupt the rule of law as an overriding principle, replacing it with security.[3] This fact alone means that it is a vital issue for law and society. The keywords here are "intensification" and "expansion" as many existing tendencies were reinforced in the aftermath

1 David Lyon, *Surveillance after September 11* (Cambridge: Polity Press, 2007).

2 See generally Magnus Hornqvist, "Risk Assessments and Public Order Disturbances: New European Guidelines for the Use of Force?" *Journal of Scandinavian Studies in Criminology and Crime Prevention* 5, 1 (2004).

3 Richard Ericson, "Ten Uncertainties of Risk-Management Approaches to Security," *Canadian Journal of Criminology and Criminal Justice* 48, 3 (2007): 345–56

Canadian Journal of Law and Society / Revue Canadienne Droit et Société, 2012, Volume 27, no. 3, pp. 291–300.

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

of 9/11, which cumulatively expanded the scope and intensity of surveillance. Three types of developments are particularly important: the technological, the military, and the corporate. Each of these has surveillance implications.

One, *technological* solutions are sought for political problems as technological means are favoured over conventional labour-intensive police work. The personal data suited to such systems are sought promiscuously and voraciously. Two, such attacks are seen as a declaration of war, requiring a *military* response, rather than crimes requiring a criminal justice response. Military surveillance methods (e.g., drones, interception of messages) are deployed, and military budgets take on a surveillance emphasis, reinforcing a doctrine that exceptional circumstances justify almost any means. Three, commercial and *corporate* entities are engaged as partners with government authorities. Corporate bodies have become increasingly involved, directly and indirectly, in surveillance, offering expertise and contributing to policy, despite the fact that they typically have even less oversight than government security agencies. The security-surveillance-industrial complex was empowered by 9/11.[4] This may also be seen, for instance, in the greatly increased funding to the Communications Security Establishment in Canada, including a one billion dollar new Ottawa headquarters[5] and a budget that has doubled since 9/11. Significant aspects of this are discussed in this special issue by Walby and Anaïs.

The decade since 9/11 has been a bonanza for corporations dealing in surveillance technologies. New systems have proliferated since 9/11, from attempts to "connect the dots" through data sharing and data mining, to camera surveillance, full body scanners, wider use of Passenger Name Records by border agencies, international data sharing, and ID cards and enhanced driver's licences.[6] Then there are the many ways in which revitalized "urban security" reflects 9/11 priorities, with, for example, restricted access and more policing at organized events,[7] and how everyday information, such as that gleaned from social media, is now appropriated for security-related surveillance.[8]

The decade since 9/11 has been marked by government-prompted and media-amplified anxiety and the growth of a culture of suspicion. True, the odds of dying in a road accident or crossing the street are vastly higher than from a terrorist attack. Yet security-surveillance policy is often guided by and spreads fear,[9] affecting negatively the lives of many, especially in

4 Lyon, *Surveillance after September 11*; Kirstie Ball and Laureen Snider, eds., *The Surveillance-Industrial Complex: A Political Economy of Surveillance* (London: Routledge, forthcoming June 2013).

5 Colin Freeze, "Canada's Little-Known Spy Agency Comes Out into the Open," *The Globe and Mail* (August 23, 2012), http://www.theglobeandmail.com/news/national/canadas-little-known-spy-agency-comes-out-into-the-open/article4260580/?page=all.

6 See, e.g., Dana Priest and William Arkin, "Top Secret America," a special series for *The Washington Post* (2010), http://projects.washingtonpost.com/top-secret-america/.

7 Stephen Graham, *Cities under Siege: The New Urban Militarism* (London: Verso, 2010).

8 Daniel Trottier, "Policing Social Media," *Canadian Sociological Review* 49, 4 (2012).

9 David Altheide, *Terrorism and the Politics of Fear* (Lanham, MD: Altamira, 2006).

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

certain population groups—and particularly male Muslim Arabs. A public fear of surveillance also chills communication and political debate, as Sunny Hughes discusses in her article, this time in a US context. It may be unnecessary to add that the funds fed to national security vastly outstrip those that might be spent on road safety.[10]

Reflecting on Security-era Surveillance

Public discourse since 9/11 has frequently resorted to questions of finding "balance" between privacy and security or assertions that "if you have nothing to hide you have nothing to fear." But these are shallow notions that require reflections and critique. The assumptions guiding post-9/11 security and surveillance policy should be scrutinized and assessed if real reflection is to occur. After all, as Lisa Austin reminds us in her article in this special issue, "due process" has suffered seriously in the Canadian context since 9/11. To reflect on these matters is an ethical endeavour in the sense that it involves trying to disclose what is actually being done through surveillance. By way of introducing these issues, three paradoxical dimensions are highlighted.

The takeover paradox

Commitment to "pre-crime" or preemption produces early intervention and social sorting and minimizes civil liberties. This is a paradox because although the practice is "pre-crime" (no law is broken yet), suspects are treated as if they are criminals. A "pre-crime" approach (popularized by the film *Minority Report*) achieved a central position among security professionals in seeking "national" security (which in any case has become increasingly blurred with domestic security). As a result, the post-crime logic of calling to account and censure and placing sanctions on wrongdoers is replaced by the pre-crime logic of security,[11] which warrants earlier intervention and curtailing civil liberties. This also produces categorical suspicion, based on profiling, and less concern with ordering of priorities when everything can be monitored at low cost.

The pre-emption of terrorism was new in the Canadian Anti-Terrorism Act (ATA). Extraordinarily, the ATA allowed police to arrest and hold a suspect for up to three days. This provision was never invoked, but the present Canadian administration would like to restore these clauses, which had a five-year sunset. But "takeover" or pre-crime practices now occur in Canada as elsewhere under the banner of security. Because gathering personal data, identification, data analysis, and profiling are vital to this,[12] surveillance is increasingly designed into the architectures of everyday life.

---

[10] See, e.g., Chris Hellman, "Has the Pentagon's Post-9/11 Spending Spree Made Us Safer?" *The Nation* (August 16, 2011), http://www.thenation.com/article/162803/has-pentagons-post-911-spending-spree-made-us-safer/.

[11] Lucia Zedner, *Security* (London: Routledge, 2009), 73.

[12] See David Skillicorn, "Understanding Complex Datasets: Data Mining with Matrix Decompositions," *International Statistical Review* 76, 1 (2008).

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

The targeting paradox

Following the pre-crime logic, and given the technical means of monitoring, everyone becomes a suspect. The paradox is that this is "total targeting," which clearly is an oxymoron. Throughout the decade since 9/11, the government's powers of surveillance have expanded dramatically, in line with the pre-emptive approach. They are directed not just at people suspected of wrongdoing, but at all citizens.[13] Phone calls, e-mails and website visits, financial records, travel itineraries, and digital images captured on cameras are swelling the mountain of data that is being mined for suspicious patterns and associations. This can be seen in the current desire by security officials to secure "total information awareness" (TIA), which was an early outcome of the "information is power" mentality underlying US approaches to security (and inscribed in the TIA logo), and as Monahan and Regan point out in their contribution to this issue, in the "fusion centres" whose purpose is to collate and coordinate data processing and sharing.[14]

The transparency paradox

It is often said that today's surveillance produces a "new transparency" in which our lives are more and more visible to organizations.[15] The paradox post 9/11 is that while we have become more transparent to organizations, they have become less transparent to us. As in the United States, where secrecy and the use of classified information has mushroomed,[16] in Canada, too, secrecy has deepened. While we are all more transparent to surveillance organizations, the converse is not true. They are opaque and veiled in operational secrecy as Walby and Anaïs point out. They also typically use sophisticated software and statistical tools that make it difficult to develop a general understanding of how surveillance operates.

We simply do not know all that is going on in domestic and international intelligence sharing and surveillance. How exactly do police, intelligence agencies, customs, financial intelligence, and foreign affairs departments share information about suspected terrorists, and where do they obtain those data in the first place? From circumstantial evidence and freedom of information requests, it is clear that they come from social media, data brokers, and the like. Particularly when it comes to personal data crossing the Canadian border into the United States, prohibitions are actually minimal.[17] In addition, it would appear from several notorious cases that there is simply insufficient personal data processing accountability.

---

13 Katja Franko Aas, Helene Oppen Gundhus, and Heidi Mork Lomell, eds., *Technologies of InSecurity: The Surveillance of Everyday Life* (London: Routledge, 2008).

14 Torin Monahan, "The Murky World of '*Fusion Centres*'," *Criminal Justice Matters* 75, 1 (2009), 20–21.

15 "The New Transparency: Surveillance and Social Sorting" is the title of a SSHRC collaborative research project to which most contributors to this special issue belong.

16 See Priest and Arkin, "Top Secret America," http://projects.washingtonpost.com/top-secret-america/.

17 Iris Klein, *Applying Canadian Privacy Laws to Transborder Flows of Personal Information from Canada to the United States: A Clarification* (Ottawa: Kris Klein Law Office, 2008).

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

As a case in point, many "mistakes" with personal data have been made since 9/11. The Canadian Security and Intelligence Service (CSIS) has been shown to use shady informants.[18] The sharing of personal information has led to detention and mistreatment of Canadian citizens abroad. Information obtained through torture has been sought to derail terror plots. Intelligence sharing has also put Canadian residents and citizens on watch lists or no-fly lists without any accompanying means of explanation or exoneration (this to an extent even in Canada where the Passenger Protect scheme set up an "Office of Reconsideration"). Authorities continue to share information with foreign governments, and once there, Canadian authorities, not to mention the individuals concerned, lose control over it.

Three Current Trends

The following description of three trends in Canadian security and surveillance practices illustrates the foregoing points.

From checking objects to prohibiting persons

At airports, there is evidence of increasing interest in *persons* as well as in potential weapons, and this also leads to increased surveillance, categorical suspicion, and profiling. This is seen, for example, in the growing use of ePassports, discussed in this volume by Brenda McPhail and others, but also in the use of "behavioural observation," which is imported from Israeli practices at Ben Gurion Airport and, one might surmise, related to the Israel-Canada Security Agreement signed by Stockwell Day and Avi Dicter in 2008. Part of that strategy is to export from Israel universally applicable "surveillance technology" that is supposedly politically neutral. The evidence suggests, however, that this technology is not neutral.[19]

Seen in a socio-economic and political context, those technologies are the product of the Israeli experience of controlling Palestinians.[20] Unfortunately, ethnic, religious, and racial profiling is entailed in their use. Even with the best intentions, Arabs and Muslims have been singled out in North America for disproportionate attention, which at worst has produced egregious situations of extraordinary rendition and the denial of human rights. Importantly, as Abu Laban and Baken show in their article, at an everyday level, the Middle East conflict also has repercussions in Canada where words and affiliations are monitored in the hope of revealing potential "terrorist" situations or allegiances.

The reason for these initiatives is that profiling is observing, recording, and analyzing selected characteristics in order to predict future behaviour. But if data are inadequate or analysis faulty, mistakes occur. What is often

---

18 Janice Tibbits, "A Decade On," *Canadian Lawyer Magazine* (September 2011).

19 See, e.g., Reg Whitaker, "Behavioral Profiling in Israeli Aviation Security as a Tool for Social Control," in *Surveillance and Control in Israel/Palestine,* ed. Elia Zureik, David Lyon, and Yasmeen Abu Laban (London: Routledge, 2010).

20 Elia Zureik, David Lyon, and Yasmeen Abu Laban, eds., *Surveillance and Control in Israel/Palestine* (London: Routledge, 2010).

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

referred to in almost childishly simple terms as "connecting the dots" is far from simple. Prior modelling is also problematic here but vital for telling "signals" from "noise." After all, terrorists may be women, "home-grown," or non-Muslim. Behavioural profiling may be viable,[21] but it is also highly controversial because of its obviously questionable human rights and civil liberties dimensions.

From "smart borders" to "perimeter security"

In August 2011, reports released by Foreign Minister John Baird indicated what is happening in so-called perimeter security.[22] It reveals that, among other things, the Air Transport Association of Canada (ATAC) supports merging Canada's no-fly list, the Passenger Protect Program, with the US Transportation Security Administration's Secure Flight program, a system that matches watch list data, into a single North American "no-fly" list inside a future continental security perimeter. The scheme was publicly announced in February 2012.[23]

We also learn in the original documents that David F. Goldstein, president of the Tourism Industry Association of Canada, said in a "modern context" information on passengers is going to be shared, and there is not much that can be done about that without affecting economic growth. Greater Toronto Airports Authority spokesperson Scott Armstrong says the reason his organization is in favour of aligning passenger data is that many travellers are actually looking to speed up their experience at airports. "If you can streamline the passenger process, obviously the quicker passengers can get through the airport the more efficient we can be, and the more efficient people can be in terms of how they allocate their time," he said.[24]

On the other hand, "concerned individuals" who were consulted "generally questioned the need to share more information, and they sought assurance that any information sharing would be governed by Canadian privacy laws and that practices and procedures would respect the due process of law and Canada's civil liberties." They "generally questioned the need to share more information, and they sought assurance that any information sharing would be governed by Canadian privacy laws and that practices and procedures would respect the due process of law and Canada's civil liberties."[25]

Speaking in an earlier phase of this process, the "Security and Prosperity Partnership," and noting the growth of corporate profits in the security

---

21 Whitaker, "Behavioral Profiling."

22 *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness* (Declaration by the Prime Minister of Canada and the President of the United States of America, February 4, 2011, Washington, DC).

23 Embassy of the United States, "Beyond the Border, One Year Later" (February 10, 2012), http://canada.usembassy.gov/news-events/2012-news-and-events/february-2012/10-february-2012-beyond-the-border-one-year-later.html; David Goldstein, *What Canadians Told Us: A Report on a Consultation on Perimeter Security and Economic Competitiveness between Canada and the United States* (Ottawa: Government of Canada, 2012).

24 Goldstein, *What Canadians Told Us.*

25 Ibid.

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

industries and the offer from police to protesters that they allow their views to be expressed in a handy "video tent," Naomi Klein noted, "Security is prosperity; surveillance is democracy."[26]

From open communications to a securitized Internet

The question of (un-) "Lawful access" was to be brought before the Canadian Parliament in 2011. Under three bills originally bundled into an "Omnibus Crime Bill" package, Internet service providers (ISPs) would be required to release personal data without warrant, for "security" reasons, thus themselves taking on a police function. Alex Himelfarb, once a senior figure in Public Safety, commented that this will make Canada meaner, not safer.[27]

These pieces of legislation grow out of Bills C-50, C-51, and C-52 from the last session of the previous Parliament, the "lawful access" technical surveillance bills. The federal and provincial Privacy Commissioners have voiced grave concerns collectively in a letter to Deputy Minister of Public Safety, and a media campaign on television and the Internet called "Stop Online Spying" has been mounted to raise awareness of the far-reaching consequences of passing such legislation.

Critics argue that Canadians' ISPs, social networks, and even their smartphones and cars will be turned into tools to spy on their activities if Bill C-51 becomes law. Minimal and inadequate oversight is in place to ensure that the powers allotted in these bills are not abused. Clause 16 of former Bill C-52 will allow law enforcement to force identification of anonymous online Internet users, even where there is no reason to suspect the information will be useful to any investigation. The same Bill would pave the way to categorical secrecy orders that will further obscure how the sweeping powers granted in it are used and seriously hinder the ability to challenge future abuses of these powers in court. In addition, the potential scope of some of its provisions could impose warrantless identification requirements on telecommunications services such as blogs and social networking sites, and could make end-to-end encryption illegal in Canada.

As Michael Geist shows, if these measures go through, ISPs will provide personal data to police without warrant or court oversight, networks will be obliged to configure themselves for real-time surveillance, and police will have new powers to obtain access to those data.[28] In the early part of 2012 these measures (now known as Bill C-30) were introduced in Parliament and created major controversy, with Privacy Commissioners, leading newspapers, and the non-governmental organization (NGO) OpenMedia.ca attacking the proposed legislation for its alleged weaknesses and its openness to police and security abuse.

---

[26] Naomi Klein, "Big Brother Democracy," *The Nation* (September 10, 2007), http://www.thenation.com/article/big-brother-democracy/.

[27] Alex Himelfarb, "A Meaner Canada: Junk Politics and the Omnibus Crime Bill," *The Métropolitain* (June 10, 2011), http://www.themetropolitain.ca/articles/view/987.

[28] Michael Geist, "Web Surveillance Legislation Requires Study, Not Speed" (2011), http://www.michaelgeist.ca/content/view/5808/135/.

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

Rethinking security-era surveillance

Nothing was inevitable in the security and surveillance responses to 9/11, and nothing is inevitable now. To rethink such major public issues is to engage ethically and to participate politically. Surveillance Studies provides analytic resources for evidence-based policy, but it is also inherently ethical. The idea of disclosive ethics has the potential to disrupt both *fatalistic* (it has to be this way during a state of exception) or *protected* (corporate-government approach, combined with secrecy and opaqueness) models and modes of surveillance.[29]

What Should Be Rethought?

One of the first questions that needs to be rethought is why surveillance is used in security initiatives. Rather than seeing surveillance as an end in itself, we should seek to encourage *human* flourishing and *human* security. This would entail recognizing that data are not merely abstract but pertain to living persons. It would open a space to consider the alternatives to a society permeated by fear, suspicion, and security and regain respect for the rule of law and for meaningful relationships and openness.

Secondly, the obsession with technology should also be reconsidered. "In technology we trust" is the underlying faith seen in the dot.com boom-bust and quest for other profits in computer and information technology.[30] But the application of technology, if not accompanied by careful oversight and accountability measures, reinforces bureaucracy's morally blind stress on efficiency. Basic questions always should be addressed when dealing with so-called technological solutions: One, are they needed at all? Two, if they are, under what conditions and with what limits?

Third, the practices of surveillance, currently focused on social sorting (and, especially since 9/11, categorical suspicion) and privacy invasion, should be recalibrated to require or permit anonymizing techniques, opt-in options, and genuine transparency about things like where data are sent. Surveillance in the service of security is neither inappropriate nor inadvisable. It is necessary. But how it is done is crucial to human outcomes.

Above all, such practices not only need to be contextualized in the frame of human purposes but also, most importantly, must have a culture of accountability and the oversight of organizations built-in from the start. This is needed at every level, and it is where political participation is crucial.

Judge Dennis O'Connor, leader of the Arar Inquiry, concluded that greater scrutiny of the security community and better-organized and more responsible information sharing between counter-terrorism bodies is needed. Arar's arrest and rendition was based on faulty information passed to the United States. O'Connor recommended that the Royal Canadian

---

[29] See Eric Stoddart, *Theological Perspectives on the Surveillance Society* (London: Ashgate, 2011).

[30] Vincent Mosco, *The Digital Sublime* (Cambridge, MA: MIT Press, 2004).

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

Mounted Police (RCMP) Commission for Public Complaints should be revamped to review all RCMP national security activities (this process currently depends only on voluntary cooperation). O'Connor also proposed that the Security Intelligence Review Committee, which oversees the Canadian Security Intelligence Service, be given expanded power to review national security activities when they involve Citizenship and Immigration or the Department of Foreign Affairs and International Trade.

The rapidly burgeoning culture of surveillance tears at the social fabric with its divisive stress on suspicion, its debilitating emphasis on fear, and its protective carapace of secrecy. As the Office of the Privacy Commissioner report *A Matter of Trust* observes, "Trust between citizens and their neighbours, as well as citizens and the state, hinges on a mutual understanding or consensus about the need to provide security protection and the need to respect rights like privacy and to preserve the free and democratic society which we all cherish."[31]

In the end, the kind of social and legal analysis engaged here should help us answer the question, what sort of society do we want? One in which fear and suspicion rule, or one where there is accountability, care with personal information, and a return to targeting only actual suspects and to evidence-based policy? What are we trying to achieve? By what means? Will we continue to allow misleading mantras such as "nothing to hide, nothing to fear" and "balancing civil liberties/privacy and security" or "you have to pay in privacy for security" to rule? Even more than a decade after the attacks there are many significant issues that need to be addressed pertaining to the surveillance legacies of 9/11.

As indicated above, the articles in this issue approach from several different angles the urgent questions surrounding what might be called "post-9/11 surveillance practices." They focus on some of the most pressing matters confronting Canadians concerned about surveillance in a post-9/11 context and offer insight and analytic depth to questions that are all-too-often given less consideration and credence than they deserve. The hope beyond all this is that the rapidly and apparently inexorably expanding net of surveillance could contract drastically, to specific and appropriate proportions, based on other guiding principles than those currently framing much of the debate.

David Lyon
Surveillance Studies Centre
Queen's University
Kingston, ON K7L 3N6
lyond@queensu.ca

[31] Office of the Privacy Commissioner, *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century* (Ottawa: OPC, 2010), http://www.priv.gc.ca/information/pub/gd_sec_201011_e.asp.

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press

Kevin D. Haggerty
Department of Sociology
University of Alberta
Edmonton, AB T6G 2H4
kevin.haggerty@ualberta.ca

https://doi.org/10.1017/S0829320100010516 Published online by Cambridge University Press