Article

Gerrymandering the National Security Narrative: A Case Study of the Canadian Security Intelligence Service's Handling of its Bulk Metadata Exploitation Program

Patrick Laurin

Laval University, Canada
patrick.laurin.4@ulaval.ca

Abstract

In November of 2016, the Federal Court of Canada published a scathing ruling pertaining to some of the Canadian Security Intelligence Service's (CSIS) big data surveillance activities. Among other charges of wrongdoing, the ruling accused the agency of not having been forthcoming with the Court about the existence of its "Operational Data Analysis Center" (ODAC), an advanced analytics bulk metadata exploitation program that had been operational since 2006. The ruling also revealed that a significant portion of the metadata collected by CSIS should not have been *retained* in ODAC, a practice that the ruling declared illegal. Drawing from the ruling, a series of classified CSIS documents obtained via requests made under the Access to Information Act, various public reports from both CSIS and the Security Intelligence Review Committee, as well as a Senate Committee hearing transcript, this article examines CSIS's conduct, justifications, and statements relating to its bulk metadata retention activities spanning from the year of ODAC's inception in 2006 to the publication of the ODAC ruling in 2016. The paper demonstrates how CSIS engaged in various forms of secrecy and how it successfully constructed and disseminated its own big data related language to effectively "gerrymander" the national security narrative, thereby ultimately ensuring its tight control over the knowledge that the Court would have of big data surveillance and CSIS's engagement with it. This would enable the Service to keep its metadata exploitation program out of sight and operational for ten years until the Court ended up declaring a significant portion of ODAC illegal in 2016.

Introduction

Over the last twenty years, intelligence agencies have gradually integrated "big data" analytics into their surveillance practices so that virtually all of them now engage in what is commonly referred to as "big data surveillance" (BDS). Unsurprisingly, scholarly interest in the matter has followed suit. This is especially true since 2013, as the Snowden revelations would lead to the publication of a slew of academic articles and books about the ins and outs of government agencies' engagement in BDS related practices, namely those involving questionable, if not downright illegal, conduct. While much has been said about the "what" and the "how" of these practices, less has been said about the ways in which agencies tend to *frame* such practices in real-time or after they are made public.

In November of 2016, the Federal Court of Canada (FCC) published a scathing ruling pertaining to some of the Canadian Security Intelligence Service's (CSIS) BDS activities. Among other charges of wrongdoing, the ruling accused the agency of not having been forthcoming with the Court about the existence of its "Operational Data Analysis Center" (ODAC), an advanced analytics bulk metadata exploitation program

Laurin, Patrick. 2020. Gerrymandering the National Security Narrative: A Case Study of the Canadian Security Intelligence Service's Handling of its Bulk Metadata Exploitation Program. *Surveillance & Society* 18 (3): 370-386.

<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2020 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#)

that had been operational since 2006. The ruling also revealed that a significant portion of the metadata collected by CSIS should not have been *retained* in ODAC, a practice that the ruling declared illegal.

Drawing from various documentary sources as bases for analysis—including the 2016 ODAC related FCC ruling, twenty CSIS classified documents relating to ODAC and/or the Service’s bulk data exploitation activities from 2006 to 2016 (i.e., four internal memorandums, five letters from CSIS management to the Minister of Public Safety and Emergency Preparedness, one privacy impact assessment, one document describing procedures relating to dataset collection and management, five communications from management to employees, two PowerPoint presentations, and two media relations documents) obtained via requests made under the Access to Information Act (ATIA), twelve CSIS public reports and twelve annual reports from the Security Intelligence Review Committee (SIRC) spanning from 2006 to 2018, as well as a Senate committee transcript—this article examines CSIS’s conduct and statements relating to its bulk metadata retention activities spanning from the year of ODAC’s inception in 2006 to the publication of the ODAC ruling in 2016.

This paper demonstrates how CSIS engaged in various forms of secrecy and how it successfully constructed and disseminated its own BDS language to effectively “gerrymander” the national security narrative relating to BDS, thereby ultimately ensuring its tight control over the knowledge that the FCC would have of BDS and CSIS’s engagement with it. This would enable the Service to keep its metadata exploitation program out of sight and operational for ten years until the FCC ended up declaring a significant portion of ODAC’s activities illegal in 2016.

This article is divided into four parts. First, CSIS is conceptualized as a particularly powerful actor in a post-9/11 world, one whose prominent role as a defender of Canadian national security renders it capable of controlling and shaping the narrative insofar as matters of national security are concerned. Namely, it does so by resorting to secrecy and what I call “category manipulation strategies” theorized as conducive to national security narrative control. After inquiring as to how this control dynamic may apply to the realm of BDS more specifically, the second part of the article consists of a chronological and analytical account of the ODAC case using the theoretical tools outlined in the first section. Third, I discuss the role played by secrecy and category manipulation in CSIS’s control over the narratives accessible to the FCC pertaining to ODAC and BDS related issues more generally. I conclude by highlighting how the case at hand raises important concerns relating to the blinding power of the current national security discourse and those like CSIS who are seen to represent it as well as the various threats presented to democratic rights and to the rule of law. To address these concerns, I propose that authorities be armed with the tools to detect the narrative control devices deployed by CSIS so that ODAC-like scenarios do not reoccur.

Controlling the Narrative of National Security

Today, the power of national security is such that “any ‘serious’ discussion [about it] cannot include skepticism about the phrase itself or the series of concepts it refers to (terrorism, secrecy, vulnerability, global threats and the like)” (Leman-Langlois 2018: 558). This is especially true since 9/11, as the “war on terror” came to unambiguously elevate national security imperatives to the top of Western policy agendas, oftentimes to the detriment of ideals promoted by other, somewhat antithetical, discourses, such as those defending democratic rights and freedoms (Ericson 2007: 36–71; Laurin 2018: 117). In Canada, this national security turn has, in part, meant that intelligence agencies have greatly extended their reach (Bell 2006)—that is, they have been targeting and monitoring an ever-growing amount of people, places, social categories, events, and practices in an ever-growing number of ways (e.g., MacMahon 2005; Molnar and Parsons 2016; Walby et al. 2016; Bennett et al. 2014: 151–168; Manzoor 2018; Lyon 2014). Among these agencies is CSIS.

The Post-9/11 Empowerment of CSIS

CSIS is a civilian government agency whose role it is “to investigate [i.e., to collect and analyze information relating to] activities suspected of constituting threats to the security of Canada. [Since 2015], CSIS may also take measures to reduce threats to the security of Canada in accordance with well-defined legal requirements and Ministerial direction” (CSIS 2019). Along with the rise in influence of national security imperatives, CSIS’s role was quite dramatically enhanced following the 9/11 terrorist attacks. For instance, Canada’s first-ever official national security policy, published in 2004, specifically deemed CSIS responsible for the management of the country’s new “Integrated Threat Assessment Centre” (ITAC) (Privy Council Office 2004: 18)—renamed the “Integrated Terrorism Assessment Centre” in 2011—a US-style “fusion center” meant to centralize and coordinate intelligence gathered by multiple government agencies in order to assess the terrorist threat.

Meanwhile, the Service’s annual budget, which had fallen from \$229 million to \$196 million between 1993–1994 and 2000–2001—a 14% decrease over a span of eight years—was increased from \$196 million to \$430 million between 2000–2001 and 2007–2008—a 120% increase over the same amount of time—only to grow by an additional 20% between 2007–2008 and 2015–2016 with only a few minor dips throughout (Canadian Security Intelligence Service 2016c, 2010b, 1992, 2006b).

CSIS has also benefited from substantial legislative changes aimed at strengthening Canada’s national security. For instance, the 2015 Protection of Canada from Terrorists Act enabled the Federal Court to issue warrants for CSIS’s out-of-country spying activities *for instances in which such activities violated foreign or international law* (Forcese 2015). Also in 2015, the controversial Anti-terrorism Act (Bill C-51) gave CSIS the unprecedented power to “disrupt” suspected security threats *before* they had a chance to come to fruition (see Zimonjic 2016a).

Finally, until recently—that is, prior to a regulatory push primarily driven by the 2017 creation of Canada’s National Security and Intelligence Committee of Parliamentarians (NSICP) as well as by the 2019 passage of Bill C-59—it would not have been controversial to argue, as many scholars have, that the oversight mechanisms meant to hold CSIS accountable for its actions had been weakened over the course of the last two decades (Forcese and Roach 2015: 399–448; Roach 2015), thus indirectly expanding the Service’s operational range. This “weakening of accountability” critique applies to CSIS’s main review body, the Security Intelligence Review Committee (SIRC)—replaced by the National Security and Intelligence Review Agency (NSIRA) in 2019 with the passage of Bill C-59—which, according to Forcese and Roach (2015: 44), “ha[d] been short-handed, under-resourced, and dogged with controversy...” (see also Shore 2006; Security Intelligence Review Committee 2004), and the breadth of its investigative powers had not been able to legally account for a growing number of CSIS’s operational practices. Another one of CSIS’s main review bodies, the Inspector General—created to act as “the ministry’s ‘eyes and ears’ on the Service”—was abruptly abolished in 2012 by the conservative government “supposedly to economize on its \$1 million a year budget...” (Forcese and Roach 2015: 44). Lastly, the FCC, which should ultimately serve as a legal shield against CSIS’s potential rights violations, has seen its power to hold CSIS accountable dwindle in recent years (Forcese and Roach 2017). Following the passages of Bills C-44 and C-51 in 2015, CSIS is now free to engage in a striking number of practices *without needing to obtain warrants from the Court* (Forcese and Roach 2015: 369, 383, 385). And, in cases where CSIS is obliged to apply for a warrant, additional legal powers have been granted to judges in some areas, thus giving them the option to approve certain warrant applications which had hitherto not been granted (Forcese and Roach 2015: 386).

Evidently, the Service has exercised its newfound resources in myriad ways, namely by significantly raising its employee counts (Canadian Security Intelligence Service 2016c, 2010b, 1992, 2006); by upgrading its infrastructure (Canadian Security Intelligence Service 2015: 53); by putting some of its newer and more invasive legal powers to use (Zimonjic 2016b); by widening its surveillance networks through new public-private partnerships (Bennett et al. 2014: 56), international agreements (Bennett et al. 2014: 106), and increased levels of information sharing (Walsh 2016); by expanding the list of surveillance targets/categories (Monaghan and Walby 2012); and by exploiting new surveillance technologies (Canadian

Security Intelligence Service 2015: 38). Above all, CSIS has also been harnessing some of its post-9/11 power to control certain facets of the increasingly popular narrative of national security.

Theorizing National Security Narrative Control

There are two main mechanisms by which government agencies can be said to exert control over portions of a given national security narrative. The first is what Setty (2017a) calls “national security secrecy,” a concept that the author divides into three overlapping classes. The first class, which I call “non-disclosure,” speaks to the type of secrets “based on a straightforward lack of disclosure by the government” (Setty 2017a: 7), one in which the government simply does not let policymakers, civilian courts, or the public know about a policy or practice. Though non-disclosure secrecy comes in many forms, relevant to this article are *government omissions*, that is, cases in which a government actor neglects to inform a given audience of relevant pieces of information when provided with an opportunity to do so (see White 1971).

Setty’s (2017a: 7) second class of national security secrecy, which I call *obfuscation*, covers cases in which secrecy is “created or maintained based on misinformation or misleading partial disclosures by the government.” As literature on government propaganda shows, there is no shortage of obfuscation tactics used by actors within the public and private sectors. Relevant for this article, however, are the following devices:

Euphemism (see Chilton 1987; Mazid 2004; Hasegawa 2005): the use of mild or indirect words or expressions as substitutions for what one considers to be too harsh or blunt when referring to something unpleasant, embarrassing, or damning.

Abstraction: the “simplification of detail, wherein formerly concrete details are left ambiguous, vague, or undefined” (Al-Harbi 2009: 81).

Minimization through information overload (see Briant 2015: 8): bombarding one with information, the vast majority of which is either neutral or favorable to one’s image, so as to drown out, and thus downplay, the importance of information that may be unfavorable to one’s image.

Contextual opportunism: the exploitation of immediate contextual factors such that there is a higher likelihood that the content of one’s communication will be under-scrutinized or altogether ignored (see Pratkanis and Aronson 2001: 45).

Half-truth (Bardach-Yalov 2012): Statements that may be completely true in and of themselves but fail to divulge larger and more inconvenient truths to which they are intimately linked.

Deception (see Jowett and O’Donnell 2011: 18, 27): statements that are false or run counter to the truth.

Whatever the tactic, national security government agencies have been known to make use of obfuscation devices in order to conceal a truth or to push an agenda (Leman-Langlois 2018; Brunton and Nissenbaum 2015: 8; Briant 2015: 8).

According to Setty (2017b: 523), the third class of national security secrecy is what he calls “constructive secrecy”:

Constructive secrecy can be best understood as occurring when the government makes a commitment on terms that are commonly understood, but the government has a second interpretation of that commitment—kept secret from the public—that is quite different than the public understanding. Under such circumstances, the government may claim

that it has abided by its public commitment and that it is not developing secret law and policy that undermines the public commitment. (Setty 2017b: 523)

Clear-cut cases of constructive secrecy involving secret interpretations of BDS related expressions (e.g., “metadata,” “tracking,” “collection”) have come to light due to the Snowden revelations. Among the culpable entities are the US’s National Security Agency (NSA); the former US Director of National Intelligence James Clapper (Setty 2017a: 8); British intelligence agencies such as the GCHQ (Nyst 2018); and Canada’s signals intelligence (SIGINT) agency, the Communications Security Establishment (CSE) (Austin 2015; Leman-Langlois 2018).

The second major mechanism by which government agencies can be said to exert control over the national security narrative is what I call “category manipulation.” It encompasses all practices involving the *construction* (i.e., the creation and/or redefinition) of the language and/or meaning of any conceptual category as well as their successful *dissemination* to other actors. For example, Harbisher (2015: 474) points out the ways in which “Britain’s Public Authorities, the intelligence community, and key members from the private sector have come to define common activists as terrorists...,” namely through their liberal application of the label “domestic extremism” to protest groups and public dissenters. To explain how this newly constructed category was successfully disseminated to a slew of state and local actors, Harbisher (2015) points to the emergence of multi-agency, public-private partnerships in the field of British security intelligence whose dissemination power is massive compared to that of isolated agencies.

CSIS’s Manufactured Threat Categories and Big Data Secrets

In confronting the available literature and empirical data relating to CSIS, it appears that CSIS has indeed seized upon its aforementioned post-9/11 potential for national security narrative control.

Category Manipulation and Secrecy at CSIS

In terms of CSIS’s role in category manipulation, Monaghan and Walby (2012)’s study—which serves as an analytical blueprint for Harbisher’s (2015) paper—describes how the Service, through its operational and editorial control of ITAC (see above), has been successful in disseminating its newly constructed national security threat category to fellow ITAC members and beyond. This security threat category—“Multi-Issue Extremism”—is one that effectively lumps together the more traditional national security threat category of foreign terrorism with those of extremism, activism, and mere public dissent (e.g., direct action and civil disobedience) “into an aggregate threat matrix” (Monaghan and Walby 2012: 134). By achieving this, the authors suggest, CSIS has played a significant role in the “transformation [of] the... categories through which national security intelligence is produced in Canada” (Monaghan and Walby 2012: 134).

In terms of secrecy, CSIS operates under and actively promotes the necessity of working behind a thick veil of secrecy, all under the guise of national security (Penney 2010; Force and Roach 2015: 183, 187, 244; Office of the Privacy Commissioner 2014: 4). This is nothing new, as Canadian intelligence agencies in general have a long track record of claiming, sometimes excessively, the need for secrecy for national security reasons (Roach 2015). Obtaining documents from CSIS through ATIA requests has always been a notoriously arduous process, one that has often been riddled with lengthy delays and empty responses (see Clément 2015; Wark 2002; Monaghan and Walby 2012). CSIS’s publicly available annual reports have long been known to be rather vague and timid insofar as the Service’s investigative practices are concerned (Stewart 2010).

Yet, contrary to what the Service might claim is an increasingly open and transparent CSIS (see Canadian Security Intelligence Service 2016b), it is quite possible that the very opposite scenario has been underway since 9/11 (Dafnos, Thompson, and French 2016). One reason might be the aforementioned weakening of various accountability mechanisms surrounding CSIS, which has limited the amount of leaked information.

Furthermore, secrecy has increasingly become enshrined in law. Bill C-44 (2015), for instance, officially prohibits CSIS from disclosing the identity of a human source. Bill C-51 (2015) allows CSIS to use its new disruption powers provided it obtain a warrant from an FCC judge “*in a secret, one-sided proceeding*” (Forcese and Roach 2015: 6; emphasis added), something that has proven fruitful for the Service (Zimonjic 2016b).

Lastly, in the post-9/11 era, CSIS has been known to omit the disclosure of relevant details that would draw suspicion to or substantiate facts relating to its engagement in legally contentious or illegal conduct to key authorities, such as the FCC or SIRC. From 2002 to 2007, for instance, CSIS failed to disclose that it knew it was probable that Maher Arar—a Canadian-Syrian dual citizen suspected of having ties with Al Qaeda by the US, who subsequently deported him to Syria—would be subjected to inhumane treatment by the Syrians, which ended up being the case (Canada v. Commission of Inquiry 2007: 248; Tibbets 2007). In its 2006–2007 annual report, the SIRC stated that crucial documents were missing from CSIS’s records pertaining to a case which involved potential Charter rights violations on the part of the Service (Security Intelligence Review Committee 2007: 18–22). In 2009, an FCC ruling highlighted that CSIS had breached its duty of candour to the Court by representing the reliability of two suspected Al Qaeda cooperators and foreign nationals in a negative light through various omissions, thus enabling their detainment and potential deportation (Waldman 2009). Finally, in 2013, FCC Judge Richard Mosley found that CSIS had deliberately breached its duty of candour by not disclosing in its applications for Domestic Interception of Foreign Telecommunications and Search (DIFTS) warrants the fact that CSE would not only be conducting surveillance for the Service, but would also be calling upon its Five Eyes partners to conduct surveillance on the CSIS’s behalf (*X(re)*, 2013 FC 1275: 635; Bell 2013).

Though many scholars have highlighted the ways in which secrecy acts as a powerful vector of Western intelligence agencies’ control over the national security narrative (e.g., Forcese 2009; Roach 2015; Geist 2015a; Israel 2015; Clement and Obar 2015; Bamford 2008; Theoharis 2016; Nyst 2018), very few have commented on the role that category manipulation plays to that same end. As a result, there exists a lack of knowledge within the literature on security intelligence about the ways in which this mechanism is concretely exercised by intelligence agencies, let alone by CSIS, an agency that only Monaghan and Walby (2012) have examined. Nevertheless, given the above, it is likely that CSIS did indeed ramp up its control over the narrative of national security as well as the growing number of actors under its influence. And it did so in relation to several features which likely make up and define such a narrative. One of these features, as I will demonstrate, is that of BDS.

Big Data at CSIS

Big data refers to “the capacity to search, aggregate and cross-reference large data sets” (boyd and Crawford 2012: 663) as well as to the extraordinary capacity to effectively analyze such massive amounts of data (Andrejevic and Gates 2014). By using complex automated algorithmic systems capable of extracting predictive patterns and trends from often incredibly fragmented and seemingly innocuous data, a task virtually unachievable by human intervention alone, big data ultimately provides “novel forms of ‘actionable intelligence’ that emerge from the analysis of ever-expanding data sets” (Andrejevic and Gates 2014: 186; see also Gandy 2012).

Big data *surveillance*, specifically, “relies upon control over collection, storage, and processing infrastructures in order to accumulate and mine spectacularly large amounts of data for useful patterns” (Andrejevic and Gates 2014: 90). Unsurprisingly, numerous national security state actors in North America such as the Central Intelligence Agency (CIA) (Andrejevic and Gates 2014), NSA (Lyon 2015: 18–20; Fuchs and Trottier 2017), Federal Bureau of Investigation (FBI) (Bennett et al. 2014: 112; Brayne 2017), Royal Canadian Mounted Police (RCMP) (Bronskill 2017), and Communications Security Establishment (CSE) (Leman-Langlois 2018) are known to operate BDS programs. Because extremely rare yet devastating events such as terrorist attacks are said to be notoriously difficult to predict and prevent through traditional “ground-up” and targeted surveillance methods (i.e., gathering data related to a previously identified target), agencies have turned to amassing as many data as digitally possible in order for the algorithms to filter out

statistical normalcies from the noise (Leman-Langlois, forthcoming) in the hopes of identifying, predicting, and ultimately pre-empting humanly unforeseeable patterns and behaviors (Andrejevic and Gates 2014). This shift in surveillance targets from the needle to the haystack has typically involved what Lyon (2014: 2) calls an “astonishingly large scale monitoring of populations” that relies on the work of sophisticated data-extraction tools—often with direct assistance from technology industry giants such as Google and Facebook—as well as on the handing over of colossal amounts of user data by strikingly compliant telecommunications companies (Lyon 2014; Leman-Langlois 2018; Austin 2016).

This not only means “mass surveillance,” as in “the surveillance of as many people as possible,” but also that the haystack must be at its highest resolution, where “any data” becomes “good data.” With regards to communications, BDS has almost invariably included the collection of so-called “metadata,” that is, “data about data”—namely dialed phone numbers, IP addresses, locations, dates and times, and identities—peripheral to the content of a communication (Guthrie Ferguson 2017: “Metadata”). National security agencies have been known—especially since the Snowden revelations—to collect vast amounts of metadata, and it appears that CSIS is no exception.

CSIS has been operating a secret bulk metadata exploitation program, named ODAC, since 2006. Among the little information that is known about the program is the fact that the Service, along with other intelligence gathering agencies such as CSE and the Canadian Border Services Agency, obtain “massive amounts of data” from Canada’s major telecommunications companies (Leman-Langlois 2018: 551) as a result of voluntary disclosures by telecoms (Austin 2016) or of court-ordered/warrant-backed requests.

Because ODAC has proven controversial in the media (e.g., Bell 2016; Freeze and Stone 2016; Boutilier 2017; Freeze and Curry 2018) and in the courts, it has become a fascinating case study of CSIS’s influence over the narrative of national security, as the Service has scrambled to legitimize its practice.

Examining CSIS’s Management of ODAC

The story of ODAC begins in April 2006 when the program first became operational (*X(re)*, 2016 FC 1105: 8). The program’s core mission, which remained largely unchanged over the course of the ten years covered by this study, is best summarized in a 2015/2016¹ classified CSIS PowerPoint presentation titled “ODAC Analysis & Investigations” obtained via ATIA request: “[ODAC] uses analytical tools and methods to provide advanced analytical support to Service investigations through data exploitation. ODAC uses the large volumes of data collected by the Service to create and derive actionable leads” (Canadian Security Intelligence Service 2015/2016).

The specific type of data analyzed by ODAC was what the Service *initially* referred to as “metadata.” According to a July 20, 2006 letter from then CSIS Director Jim Judd to the Minister of Public Safety and Emergency Preparedness Stockwell Day, a letter whose main purpose was to inform the Minister of ODAC’s creation (obtained through ATIA request), metadata “in layman’s terms... is information that describes how, when and where a communication occurred” (Canadian Security Intelligence Service 2006a: 1). *Internally*, CSIS quite clearly differentiated metadata from the actual “content” of a communication, the latter of which was not exploited by ODAC. Metadata were *retained indefinitely* in ODAC for current and future investigative purposes. Crucially, the type of metadata retained did not only stem from information (i.e., content + metadata) collected from “targeted threats.” It also stemmed from incidentally collected “*non-threat related and third-party information*” (NTTP) (*X(re)*, 2016 FC 1105: 18–20; emphasis added), that is, *information collected from entities who are unassociated with the specific threats as defined in each of CSIS’s warrant applications*.

¹ The exact year in which the PowerPoint presentation was created and/or took place is not clear.

2006–2011: Selective Disclosure

CSIS quickly presented the ODAC program to the Minister for approval, as was its legislatively established duty. The Service had also intended to present the program to the FCC, as is made clear in the aforementioned letter: “[CSIS] also plan[s] to brief the Federal Court on this initiative [ODAC] at an appropriate juncture” (Canadian Security Intelligence Service 2006a: 2). Doing so was in line with the Service’s moral, professional, and jurisprudence-based duty of candour. Yet, this did not occur.

In fact, until late 2011, no allusion *to*, let alone any explicit mention *of*, CSIS’s metadata retention practices would ever be made to the FCC. True, CSIS did refer to ODAC in the Service’s 2007–2008 public report, stating that the “Operational Data Analysis Centre (ODAC) provides support to the Service’s operational branches by performing advanced analysis of data that is collected on subjects of investigation” (Canadian Security Intelligence Service 2008: 19–20). Upon closer analysis, however, the short statement does little besides revealing the name of the program, the veil of secrecy effectively remaining intact. First, consistent with Al-Harbi (2009)’s concept of *abstraction*, the statement is deliberately vague: that ODAC performs “advanced analysis of data” is highly ambiguous at best. Second, the *half-truthful* nature of the statement fails to provide information on both the type of data processed and the Service’s retention policy. Perhaps as a consequence of this *non-disclosure secrecy*, the report’s mention of ODAC failed to raise the FCC’s suspicion.

2011: A New Layer of Secrecy

On December 16, 2011, the FCC held a closed hearing with CSIS in order to deal with the Service’s proposed warrant template amendments. Among the changes sought was one aimed at “bettering” the language of a specific warrant condition present in some of the templates. The following is an excerpt from the 2016 ODAC ruling which quotes counsel for CSIS’s 2011 presentation of its proposed amendment:

there are other minor changes to the conditions that we think go to clarity... we also looked at trying to better the language... if I can put it that way; not change but to better the language... before it read as follows: ‘... subject to condition 1, any communication of a person’ and now we have included the words ‘the content of any communication’. So it makes it clear the metadata is not part of what would be destroyed. And just so the Court is aware, basically the metadata is not destroyed and is retained no matter what happens to the communication except for solicitor-client which will be destroyed....
(*X(re)*, 2016 FC 1105: 46)

In 2016, the Court recognized that the added detail in order to “better the language” was more consequential than it appeared. Yet, the Service managed to have it accepted as trivial by using three tactics. The first was by engaging in *contextual opportunism*. As Judge Noël himself points out in the ruling, CSIS’s clarification occurred in the context of a hearing whose purpose was unrelated to issues regarding metadata practices (*X(re)*, 2016 FC 1105: 46). Moreover, the matter, according to the judge, was addressed “in the *final moments* of the... hearing... [as a] *last minute comment*” in response to his asking counsel if it had anything else to raise (*X(re)*, 2016 FC 1105: 46, *emphases added*). Second, CSIS engaged in *minimization through information overload*. According to the judge, CSIS’s metadata/content clarification occurred at the end of the hearing “which dealt with *numerous amendments* to the warrant conditions...” (*X(re)*, 2016 FC 1105: 46; *emphases added*), thus implying that CSIS’s intervention had a higher likelihood of being lost amid the noise. Third, CSIS counsel also made obvious use of *euphemistic language*, qualifying the changes as “minor,” “stylistic,” and as mere efforts to “not change but to better the language” and to “really to reflect the practice” (*X(re)*, 2016 FC 1105: 46, 120).

Of course, as the judge points out often in his ruling, the changes sought were not innocuous. That “communication” be split into two new sub-categories, that of metadata and content, meant that “CSIS effectively rendered [the warrant] silent on [metadata]” (*X(re)*, 2016 FC 1105: 9). It in fact allowed CSIS to retain NTPP metadata, a practice that, unbeknownst to the FCC at the time, the Service had been engaging in for five years, not to mention one that the same Court would deem illegal in 2016. Yet, due to the work

of various obfuscation devices, the FCC ultimately approved the changes, thus proving the Service successful in its category manipulation efforts, that is, in disseminating and selling its freshly constructed communications categories to the FCC.

2016: The SIRC Report

Four years later, beginning in June 2015, with CSIS having yet to inform the FCC of ODAC's existence, the Court began to hold six hearings with CSIS in which the issue of NTTP metadata collection and retention was often raised by Judge Noël. Namely, the judge indicated that "warrant conditions should clearly express that non-threat, non-target information, such as third-party information, should not be retained" (*X(re)*, 2016 FC 1105: 47). Nevertheless, CSIS did not ever bring up its metadata retention policy. Instead, counsel for the Service highlighted the complexity of issues relating to retention of NTTP metadata, adding that additional time to reflect was needed. Still uninformed by CSIS about its ODAC's operations, the FCC would abide by the Service's request, granting it two extensions in the process. On December 8, 2015, CSIS submitted a letter to the Court in which several amendments to warrant conditions were proposed. Crucially, "the letter... did not divulge the Service's policy of retaining metadata" (*X(re)*, 2016 FC 1105: 47).

Less than two months later, on January 28, 2016, SIRC published its 2014–2015 annual report. The committee noted that, while CSIS did indeed refer to its metadata retention program in the 2011 closed hearing, "SIRC was given no indication that the Service was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of that discussion" (SIRC 2015: 25). SIRC thus recommended that CSIS inform the FCC of "the particulars of the Service's retention and use of metadata collected under warrant" (Security Intelligence Review Committee 2015: 25). This was the first time that the FCC would be made aware of ODAC.

It would also be the first time that CSIS would publicly defend its conduct by squarely rejecting SIRC's recommendation, stating, as paraphrased in the SIRC review, that the CSIS Act:

does not confer general supervisory authority to Federal Court judges, therefore, [CSIS] believes that SIRC's recommendation was both inappropriate and unwarranted. Moreover, the Service maintains that its position on the issue in question [retention and use of metadata collected under warrant] was communicated clearly and transparently to the Federal Court during a warrant application in December 2011. (Security Intelligence Review Committee 2015: 26; emphasis added)

Though I will later comment on the first portion of the statement, the second portion is deceptive on two levels. First, as discussed above, CSIS employed various devices which mainly served to obfuscate the visibility and minimize the importance of its 2011 amendment proposal. Second, it does not follow from the content of CSIS's 2011 proposal that the Service manages a fully operational BDS program that retains virtually all collected metadata.

On the day following the release of SIRC's report, the FCC received a letter from the Assistant Deputy AG (on CSIS's behalf) which effectively doubled down on CSIS's defense: "at the [closed] hearing of December 16, 2011 the CSIS had '*clearly communicated*... the retention program of associated data..." (*X(re)*, 2016 FC 1105: 13, emphasis added). The letter further indicated that, in a stated effort to avoid future confusion, CSIS counsel had, in its written affidavits likely submitted to the FCC somewhere in the summer of 2015, already made changes in its request for two warrant applications, changes which, the letter deceptively claimed, had already been brought to the attention of the judge in the context of the summer of 2015 closed hearings (see *X(re)*, 2016 FC 1105: 13–14). In reality, the changes were quietly added to the affidavit and ultimately concealed from the FCC's view up until the publication of the SIRC report half a year later.

The Advent of "Associated Data"

These changes added the notion of "associated data" to warrant conditions while clearly differentiating it from "content" in that *only* the former was to be retained. According to a memorandum for CSIS's director

to the minister obtained through ATIA request and dated April 11, 2016, “Associated data is information, in structured fields, linked with a communication. Examples include email addresses, telephone numbers [redacted] as well as duration, dates and times of phone calls or Internet sessions. It does not include any information that could reveal the purpose of the communication, nor any part of its content” (Canadian Security Intelligence Service 2016a: 7–8).

This is the definition also adopted by then CSIS Director Michel Coulombe and by CSIS Assistant Director of Operations Enablement John Cousineau in the months following the ODAC ruling (see Appendix 1). It also seems remarkably similar to the Service’s previous descriptions of metadata (see Appendix 2). What is more, the term “associated data” is very seldom used by anyone else, including other members of the Five Eyes intelligence community, IT professionals, and the media, let alone the general public. In fact, even for CSIS itself, the term was new. When looking at all available ODAC-related CSIS classified documents obtained through ATIA, some of which are from 2006, 2008, 2010, 2011, 2012, 2014 and 2016, the only mentions of “associated data” can be found in the 2016 documents, while those of September 26, 2014 and below use the term “metadata” when referring to similar objects. And, because we know that CSIS did indeed make use of the term “associated data” in its 2015 written affidavits aimed at amending warrant conditions, it is reasonable to believe that the term would have emerged in CSIS’s own vernacular somewhere over the course of that same year. From then on, CSIS entirely replaced “metadata” with “associated data.”

Due to incomplete access to all relevant information, it is impossible to provide a definitive explanation for the change. However, given CSIS’s history of misleading the FCC regarding ODAC, given the curious timing at which the change occurred—in 2015, around the time that the FCC was prying especially heavily into the Service’s BDS related affairs—and, finally, given the questionable secrecy under which it was made, this category manipulation change in terminology—which can be called “category rebranding” for lack of a better expression—may have been used not merely for the purpose of dissemination but also for obfuscation purposes, ultimately to preserve secrecy.

2016: *X(re)*

From February to May 2016, five closed FCC hearings took place. Besides addressing warrant amendments, these hearings mostly covered CSIS’s now controversial metadata retention activities, as Judge Noël intended. On two separate occasions, CSIS admitted that it had not been totally forthright with the FCC insofar as its metadata retention practices were concerned.

On November 3, 2016, the 135–page redacted version of FCC Judge Noël’s 2016 *X(re)* (FC 1105) ruling, which heavily based its rationale and decisions on the arguments and statements presented over the course of the five hearings, was publicly released. Though I have thus far been referring to the ruling as the “ODAC ruling,” it is worth noting that CSIS, at some point during the nine months spanning from the first hearing to the ruling’s publication, changed the name of the ODAC program (*X(re)*, 2016 FC 1105: 23), though the new appellation is unknown due to redactions in Noël’s ruling. It is not clear whether the new, “ODAC 2.0,” is the result of substantial policy and/or operational changes pertaining to CSIS’s BDS-related practices.

The ruling contains four core decisions, two of which are relevant to this paper. The first states that “[t]he CSIS has a limited mandate which does not permit the retention of associated data... as it has done so since 2006, *therefore this retention of associated data is illegal...*” (*X(re)*, 2016 FC 1105: 126, emphasis added). Note that Judge Noël’s use of the term “associated data” has a different meaning: it refers to NTTP metadata. Thus, the decision did not render *all* metadata retention illegal. The retention of target-threat related metadata would remain legal. Nevertheless, that the judge chose to use “associated data,” a bona fide CSIS creation, to refer to what he could have easily called “NTTP metadata,” especially in a context in which his own definition of “associated data” did not match that of CSIS, remains difficult to explain. Whatever the judge’s reasons may have been, however, the end result is that part of CSIS’s BDS terminology pushed its way into the FCC’s own BDS lexicon, thereby once again demonstrating the narrative control effects of category manipulation.

Judge Noël's ruling also states that "*CSIS has breached, again, the duty of candour it owes to the Court*" (*X(re)*, 2016 FC 1105: 126, emphasis added). And it has done so, the ruling argues elsewhere, "by failing to inform [the Court] clearly and transparently of its retention program, more specifically in regard to associated data collected and retained through the operation of warrants" (*X(re)*, 2016 FC 1105: 7).

Throughout the ruling, the judge lists a series of opportune moments in which CSIS could have been forthcoming with the existence and function of ODAC but was not. All but one of these occurrences has been discussed above. This instance regards CSIS's claim, initially submitted as a rebuttal to one of the SIRC 2014–2015 report's recommendations, that the CSIS Act "does not confer any general supervisory authority to Federal Court judges" (Security Intelligence Review Committee 2015: 26). As alluded to above, there are serious reasons to doubt the level of earnestness with which CSIS justified itself here. First, recall that the Service had initially (i.e., 2006) planned to present its ODAC program to the FCC. Now, however, CSIS dismissed any apparent need to do so. Second, it is quite clear that CSIS knew itself to be accountable to the FCC insofar as ODAC was particularly concerned. In a 2010 CSIS classified document obtained through ATIA request titled "Canadian Security Intelligence Service Operational Data Analysis Centre Privacy Impact Assessment," the Service states that "[t]here are several accountability mechanisms designed to shape operational activities including those of ODAC" (Canadian Security Intelligence Service 2010a: 26). Among such "control and review mechanisms and processes," which CSIS recognizes are "prescribed by the CSIS Act," is the FCC. The document then states that, in order for the Court to authorize CSIS's engagement in intrusive investigation techniques, "CSIS must provide *solid* justification for the proposed use of these techniques in an affidavit..." (Canadian Security Intelligence Service 2010a: 27; emphasis added).

The apparent contradiction between various statements regarding the supervisory role of the FCC can be resolved. Recall Director Judd's 2006 letter to the Minister which stated that "CSIS also plan[s] to brief the Federal Court on this initiative [ODAC] at an appropriate juncture" (Canadian Security Intelligence Service 2016: 2). Though, for most, the statement as a whole reads as a clear intention to notify the Court of ODAC while recognizing the FCC's purview, the non-binding and temporally ambiguous character of the terms "plan" and "appropriate juncture" stealthily provide CSIS with an "opting-out" option which allows for indefinite delay.

Such a tactic, which "bakes" a difficult to detect interpretation into an otherwise straightforward statement, is akin to what Setty (2017a: 10) calls "constructive secrecy." Based on the examination of the FCC ruling and other documentation at hand, there is no direct evidence of CSIS ever claiming that it either *had to* or *definitely would* instruct the FCC of ODAC. In other words, CSIS never actually shut the "opting-out" door that it had opened in 2006 through methods of constructive secrecy. While this certainly does not invalidate either my or Judge Noël's claims about CSIS's deceptiveness, it nonetheless makes it impossible to defend them with absolute certainty. In fact, this is perhaps part of the reason why Judge Noël's ruling does not go as far as accusing CSIS of *purposeful* breach of candour, as did Judge Mosley's 2013 ruling (*X(re)*, 2013 FC 1275) three years prior. This doesn't, however, prevent the judge from expressing his disappointment with having to acknowledge that very fact, thereby implicitly revealing his subjective opinion that CSIS likely acted deliberately: "[u]nfortunately, the evidence is inconclusive as to whether or not the CSIS intentionally did not inform the Court in a clear and transparent manner" (*X(re)*, 2016 FC 1105: 50, emphasis added).

Concretely, both ruling decisions discussed above carried with them legal consequences. From the first decision, which deemed the retention of NTTP metadata illegal, it necessarily followed that CSIS would be forced to cease all future retention of NTTP metadata. Perhaps unexpectedly, however, the ruling did not require CSIS to destroy any of its NTTP metadata obtained since 2006, citing potential jurisdictional issues and a lack of submissions on the topic from counsel on both sides (*X(re)*, 2016 FC 1105: 125). As for the "breach of candour" decision, legal consequences were more potential than actual, as the judge threatened CSIS with future contempt of Court proceedings should the Service continue to ignore the FCC's past and present calls for candour.

Discussion

In the foregoing ODAC case study, I have outlined the various secrecy and category manipulation devices with which CSIS ensured its control over the BDS related national security narrative, thus enabling itself to effectively limit and dictate the list of possible ways in which the FCC could potentially conceive of the nature, breadth, and scope of its metadata retention program and related practices.

Specifically, the analysis shows how CSIS engaged in all three forms of national security secrecy as theorized by (Setty 2017a: 7–10). First, in terms of “non-disclosure” secrecy, the Service repeatedly omitted to disclose certain highly controversial pieces of information to the FCC related to its BDS program and NTTP metadata retention practices. These rather convenient forms of government omissions, which effectively serve to conceal controversial and potentially damning information, are certainly not uncommon amongst intelligence agencies across the world, and CSIS, it seems, is no exception. In terms of “obfuscation” secrecy, it is quite clear that the Service misled the FCC on multiple occasions, and to great effect, by deploying an impressive array of techniques discussed most prominently in literature on government propaganda. By drawing from such scholarship in order to assess the degree to which CSIS engaged in obfuscation, this analysis enriches the literature on security intelligence by providing a more systematized framework from which to assess the statements made by intelligence agencies about their own conduct. Finally, the analysis also shows how CSIS engaged in “constructive secrecy,” adding the Service to a growing list of government agencies culpable of deploying the tactic (Setty 2017a: 8; Nyst 2018; Leman-Langlois 2018).

Insofar as “category manipulation” is concerned, our analysis shows how CSIS constructed and successfully disseminated two major BDS category changes to the FCC: the conceptual pulling apart of metadata from content and the rebranding of “metadata” with the newly created “associated data” label. These findings expand on the work of Monaghan and Walby (2012) and Harbisher (2015) on the possible *nature* of the national security categories that intelligence agencies may be inclined to manipulate—adding “data categories” to these authors’ “threats categories”—as well as to the possible drivers susceptible of facilitating the dissemination of national security categories—adding “secrecy tactics” to “centralized intelligence” as possible contributors.

Lastly, and perhaps most importantly, this article demonstrates how one national security narrative control mechanism may be used in order to fulfill the objectives of another. With both the conceptual dismantling of metadata and their rebranding as “associated data,” we saw secrecy devices being used for the purpose of category manipulation. And, in one of these instances, the reverse scenario was also likely at play. On the whole, these findings enrich the literature on security intelligence, which has thus far been inclined to address each major mechanism in isolation from one another. Yet, they also provide us with clues as to the existence of a hardly discussed hybrid tactic that CSIS and government agencies may use more widely to exert control over a national security narrative. This tactic, which I will call “terminological catch-me-if-you-can,” involves the changing and subsequent dissemination of new labels relating to categories and/or practices for which little to no objective change can be noted in order to conceal a truth that directly relates to said categories and/or practices. Insofar as the ODAC case study is concerned, it is quite possible, though impossible to confirm with certainty, that CSIS deployed such a tactic in its rebranding of metadata as “associated data,” or in its relabeling of ODAC (note that, since the new label is classified, ODAC 2.0 has now officially disappeared).

Conclusion

That CSIS could freely operate ODAC for ten years is concerning in more than one way. First, it exemplifies how the post-9/11 sacrosanct quality of national security can be used as “a potential smoke screen for activities that might not be conceived as security-related” (Leman-Langlois 2018: 158).

Second, the ODAC scandal highlights the problem of government secrecy, a practice which, according to Setty (2017a), has “increased dramatically” among democratic nations ever since 9/11. Secrecy limits accountability (Roach 2015), and, ultimately, “opens the door for any number of constitutional, civil, and human rights to be violated” (Setty 2017b: 514). In the case at hand, CSIS’s excessive secrecy meant that the FCC did not possess any means by which to hold CSIS accountable for ODAC. This effectively meant that the Service likely retained information on thousands of Canadians for ten years without any clear legal basis to do so.

Third, the ODAC scandal directs our attention to what is perhaps an overconcentration of power in the hands of the executive, such that CSIS is capable of singlehandedly prescribing the perspectives (i.e., categories) by which national security matters are to be understood by actors other than itself, *including those meant to hold it accountable for its actions*.

Fourth, all three cited concerns are rendered even more serious by the particular *nature* of the data kept secret and framed in a convenient matter by CSIS. This is because of how especially game-changing BDS is when compared to traditional methods of surveillance. Not only do the data-hungry and algorithmic pattern-seeking functions of BDS entail the monitoring of significantly higher counts of people and layers of data than does traditional surveillance, but they also turn the traditional legal and rights-based logics of suspicion and presumption of innocence on their head (Lyon 2015; Lubin 2018; Fairfield and Luna 2014; Tréguer 2017): everyone and everything must be scrutinized as potential suspects in order to spot the “guilty” few. Furthermore, numerous authors have criticized and issued warnings about the privacy-eroding effects of BDS (Lyon 2014; Tufekci 2014; Richards and King 2014; Andrejevic and Gates 2014; Ball, Di Domenico, and Nunan 2016; Cohen 2013). These criticisms hold true even in regards to metadata. Though perhaps unremarkable at first glance, metadata can be shockingly revealing of people’s patterns of behavior, personal relationships, movements, tastes, and so on (Lyon 2014, 2015: 71).

Given the gravity of the above concerns, it is crucial that we directly address the conditions that allow for cases such as ODAC to take place. And, though part of the explanation for ODAC’s long lifespan lies in deep secrets and flat out lack of disclosure, much of it lies in a combination of obfuscation secrecy and category manipulation. Thus, in addition to the usual calls for enhanced accountability (e.g., Forcese and Roach 2015: 38–98; Whitaker 2015; Geist 2015b; Shore 2006), we need to arm oversight and review authorities, civil liberty lawyers, parliamentarians, the media, and academics with what Austin (2015: 103–125) calls a “‘hacker’ mentality, looking for non-obvious ways to read,” in this case, CSIS’s statements or the relevant legislation upon which the Service bases its operations. That way, CSIS’s attempts to mislead authorities or to overstretch legal boundaries may be detected before it has a chance to substantiate any of the above concerns.

References

- Al-Harbi, Ahlam M. 2009. Jargonizing and Abstracting the “War on Terror”: The “Self” and the “Other” Representations. *The Linguistic Journal* 4 (2): 77–109.
- Andrejevic, Mark, and Kelly Gates. 2014. Big Data Surveillance: Introduction. *Surveillance & Society* 12 (2): 185–196.
- Austin, Lisa M. 2015. Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 103–125. Ottawa, CA: University of Ottawa Press.
- . 2016. Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints. *Theoretical Inquiries in Law* 17 (2): 451–485.
- Ball, Kirstie, Marialaura Di Domenico, and Daniel Nunan. 2016. Big Data Surveillance and the Body-Subject. *Body & Society* 22 (2): 58–81.
- Bamford, James. 2008. *The Shadow Factory: The Ultra Secret NSA from 9/11 to the Eavesdropping on America*. New York: Doubleday.
- Bardach-Yalov, Elina. 2012. Analyzing Russian Propaganda: Application of Siegfried Kracauer’s Qualitative Content Analysis Method. *Journal of Information Warfare* 11 (2): 24–36.
- Bell, Colleen. 2006. Surveillance Strategies and Populations at Risk: Biopolitical Governance in Canada’s National Security Policy. *Security Dialogue* 37 (2): 147–165.

- Bell, Stewart. 2013. Court Rebukes CSIS for 'Five Eyes' Monitoring; Spying on Suspects. *National Post*, November 26. <https://nationalpost.com/news/canada/court-rebukes-csis-for-secretly-asking-international-allies-to-spy-on-canadian-terror-suspects> [accessed January 9, 2019].
- . 2016. Secret CSIS Unit Illegally Kept Data, Court Rules. *National Post*, November 4. <https://nationalpost.com/news/politics/judge-blasts-csis-for-not-revealing-secret-program-that-illegally-kept-metadata> [accessed January 9, 2019].
- Bennett, Colin J., K.D. Haggerty, David Lyon, and Valerie Steeves, eds. 2014. *Transparent Lives: Surveillance in Canada*. Edmonton, CA: Athabasca University Press.
- Boutilier, Alex. 2017. CSIS Kept All Details in Controversial Database. *Toronto Star*, June 9. <https://www.thestar.com/news/canada/2017/06/08/csis-kept-all-metadata-on-third-parties-for-a-decade-top-secret-memo-says.html> [accessed February 10, 2019].
- boyd, danah, and Kate Crawford. 2012. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication & Society* 15 (5): 662–679.
- Brayne, Sarah. 2017. Big Data Surveillance: The Case of Policing. *American Sociological Review* 82 (5): 977–1008.
- Briant, Emma. 2015. *Propaganda and Counter-Terrorism: Strategies for Global Change*. Manchester, UK: Manchester University Press.
- Bronskill, Jim. 2017. RCMP Abandoned Metadata-Crunching Tool Used to Track Criminal Intelligence. CTV News, May 9. <https://www.ctvnews.ca/canada/rcmp-abandoned-metadata-crunching-tool-used-to-track-criminal-intelligence-1.3404566> [accessed January 21, 2019].
- Brunton, Finn, and Helen Nissenbaum. 2015. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: The MIT Press.
- Chilton, Paul. 1987. Metaphor, Euphemism and the Militarization of Language. *Current Research on Peace and Violence* 10 (1): 7–19.
- Clement, Andrew, and Jonathan A. Obar. 2015. Canadian Internet "Boomerang" Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 13–44. Ottawa, CA: University of Ottawa Press.
- Clément, Dominique. 2015. "Freedom" of Information in Canada: Implications for Historical Research. *Labour/Le Travail* 75 (1): 101–131.
- Cohen, Julie E. 2013. What Privacy Is For. *Harvard Law Review* 126 (7): 1904.
- Dafnos, Tia, Scott Thompson, and Martin French. 2016. Surveillance and the Colonial Dream: Canada's Surveillance of Indigenous Self-Determination. In *National Security, Surveillance and Terror*, edited by Randy K. Lippert, Kevin Walby, Ian Warren, and Darren Palmer, 319–342. New York: Palgrave Macmillan.
- Ericson, Richard Victor. 2007. *Crime in an Insecure World*. Cambridge, UK: Polity.
- Fairfield, Joshua, and Erik Luna. 2014. Digital Innocence. *Cornell Law Review* 99 (5): 981–1076.
- Forcese, Craig. 2009. Assessing the Secrecy Rules. *IRPP Choices* 15 (5): 1–38.
- . 2015. Bill C-44: Statement to Standing Senate Committee. *National Security Law: Canadian Practice in Comparative Perspective* (blog), March 23. <http://craigforcese.squarespace.com/national-security-law-blog/2015/3/23/bill-c-44-statement-to-standing-senate-committee.html> [accessed April 11, 2019].
- Forcese, Craig, and Kent Roach. 2015. *False Security: The Radicalization of Canadian Anti-Terrorism*. Toronto, CA: Irwin Law.
- . 2017. Bill C-51: The Good, the Bad... And the Ugly. *The Walrus*, May 4. <https://thewalrus.ca/bill-c-51-the-good-the-bad-and-the-truly-ugly/> [accessed April 11, 2019].
- Freeze, Colin, and Bill Curry. 2018. Harvesting of Ordinary Canadians' Data by CSIS Continues, Report Says. *The Globe and Mail*, June 21. <https://www.theglobeandmail.com/politics/article-in-spite-of-past-warnings-csis-continues-to-harvest-troves-of-data-on/> [accessed January 9, 2019].
- Freeze, Colin, and Laura Stone. 2016. Minister Vows Action on CSIS. *The Globe and Mail*, November 5. <https://www.theglobeandmail.com/news/national/csis-vows-changes-amid-criticism/article986548/> [accessed January 12, 2019].
- Fuchs, Christian, and Daniel Trotter. 2017. Internet Surveillance after Snowden: A Critical Empirical Study of Computer Experts' Attitudes on Commercial and State Surveillance of the Internet and Social Media Post-Edward Snowden. *Journal of Information, Communication and Ethics in Society* 15 (4): 412–444.
- Gandy, Oscar. 2012. Statistical Surveillance: Remote Sensing in the Digital Age. In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, K.D. Haggerty, and David Lyon, 125–133. New York: Routledge.
- Geist, Michael. 2015a. Introduction. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 1–9. Ottawa, CA: University of Ottawa Press.
- . 2015b. Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 225–255. Ottawa, CA: University of Ottawa Press.
- Guthrie Ferguson, Andrew. 2017. *The Rise of Big Data Policing*. New York: New York University Press.
- Harbisher, Ben. 2015. Unthinking Extremism: Radicalising Narratives That Legitimise Surveillance. *Surveillance & Society* 13 (3/4): 474–486.
- Hasegawa, Hiroshi. 2005. Euphemism in English and Japanese: A Pragmatic Contrastive Study. PhD diss., University of Tasmania.
- Israel, Tamir. 2015. Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 71–101. Ottawa, CA: University of Ottawa Press.
- Jowett, Garth S., and Victoria O'Donnell. 2011. *Propaganda and Persuasion*, 5th ed. Los Angeles, CA: Sage.

- Laurin, Patrick. 2018. Dompter le futur au 21^e siècle: Discours politiques canadiens sur la gouvernance de la sécurité publique. PhD diss., University of Ottawa.
- Leman-Langlois, Stéphane. 2018. State Mass Spying as Illegalism. *Critical Criminology* 26 (4): 545–561.
- . Forthcoming. Big Data Against Terrorism. In *Security Intelligence and Surveillance in the Big Data Age: The Canadian Case*, edited by David Lyon and David Murakami Wood. Kelowna, CA: UBC Press.
- Lubin, Asaf. 2018. “We Only Spy on Foreigners”: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance. *Chicago Journal of International Law* 18 (2): 502–552.
- Lyon, David. 2014. Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society* 1 (2): 1–13.
- . 2015. *Surveillance after Snowden*. Cambridge, UK: Polity Press.
- MacMahon, Sean F. 2005. We Are All Potential Terrorists Now: The Reconstitutive Effects of the Anti-Terrorism Act and the USA Patriot Act. *Review of Constitutional Studies* 10 (1-2): 46–72.
- Manzoor, Muhammad Asif. 2018. Real-Time Vehicle Make and Model Recognition System. PhD diss., University of Regina.
- Mazid, B. M. 2004. “Sharp Wits and Fine Phrases”: Euphemism and Dysphemism in the War-on-Iraq Discourse. *IJAES* 5: 171–188.
- Molnar, Adam, and Christopher Parsons. 2016. Unmanned Aerial Vehicles (Uavs) and Law Enforcement in Australia and Canada: Governance through “Privacy” in an Era of Counter-Law? In *National Security, Surveillance and Terror*, edited by Randy K. Lippert, Kevin Walby, Ian Warren, and Darren Palmer, 225–247. New York: Palgrave Macmillan.
- Monaghan, Jeffrey, and Kevin Walby. 2012. Making up “Terror Identities”: Security Intelligence, Canada’s Integrated Threat Assessment Centre and Social Movement Suppression. *Policing and Society* 22 (2): 133–151.
- Nyst, Carly. 2018. Secrets and Lies: The Proliferation of State Surveillance Capabilities and the Legislative Secrecy Which Fortifies Them – An Activist’s Account. *State Crime Journal* 7 (1): 8–23.
- Penney, Steven. 2010. National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits. *Osgoode Hall Law Journal* 48 (2): 247–286.
- Pratkanis, Anthony R., and Elliot Aronson. 2001. *Age of Propaganda : The Everyday Use and Abuse of Persuasion*, 2nd ed. New York: W.H. Freeman.
- Richards, Neil M., and Jonathan H. King. 2014. Big Data Ethics.(Internet Privacy Regulation). *Wake Forest Law Review* 49 (2): 393–432.
- Roach, Kent. 2015. Permanent Accountability Gaps and Partial Remedies. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 163–203. Ottawa, CA: University of Ottawa Press.
- Setty, Sudha. 2017a. *National Security Secrecy*. Cambridge, UK: Cambridge University Press.
- . 2017b. The President’s Private Dictionary: How Secret Definitions Undermine Domestic and Transnational Efforts at Executive Branch Accountability. *Indiana Journal of Global Legal Studies* 24 (2): 513–546.
- Shore, Jacques JM. 2006. Intelligence Review and Oversight in Post-9/11 Canada. *International Journal of Intelligence and CounterIntelligence* 19 (3): 456–479.
- Stewart, Brian. 2010. CSIS and the Lure of Secrecy. *CBC News*, June 10. <https://www.cbc.ca/news/canada/csis-and-the-lure-of-secrecy-1.919255> [accessed March 5, 2019].
- Theoharis, Athan. 2016. Expanding U.S. Surveillance Powers: The Costs of Secrecy. *Journal of Policy History* 28 (3): 515–534.
- Tibbets, Janice. 2007. Arar’s Torture, Deportation Forewarned; Declassified Sections of Report Cast Blame on CSIS. *Calgary Herald*, August 10. <https://www.pressreader.com/canada/calgary-herald/20070810/textview> [accessed January 9, 2019].
- Tréguer, Félix. 2017. Intelligence Reform and the Snowden Paradox: The Case of France. *Media and Communication* 5 (1): 17–28.
- Tufekci, Zeynep. 2014. Engineering the Public: Big Data, Surveillance and Computational Politics. *First Monday* 19 (7). <http://dx.doi.org/10.5210/fm.v19i7.4901>.
- Walby, Kevin, Randy Lippert, Ian Warren, and Darren Palmer. 2016. Interrogating National Security, Surveillance, and Terror in Canada and Australia. In *National Security, Surveillance and Terror*, edited by Randy K. Lippert, Kevin Walby, Ian Warren, and Darren Palmer. New York: Palgrave Macmillan.
- Waldman, Lorne. 2009. Troubling Lack of Candour by CSIS; Spy Agency Has Abused Power by Providing Tainted Testimony in Secret Hearings. *Toronto Star*, July 14. https://www.thestar.com/opinion/2009/07/14/troubling_lack_of_candour_by_csis.html [accessed January 9, 2019].
- Walsh, Patrick F. 2016. Australian National Security Intelligence Collection since 9/11: Policy and Legislative Challenges. In *National Security, Surveillance and Terror*, edited by Randy K. Lippert, Kevin Walby, Ian Warren, and Darren Palmer, 51–74. New York: Palgrave Macmillan.
- Wark, Wesley. 2002. Canada’s Access to Information Act and the Canadian Security and Intelligence Community. Canadian Intelligence Resource Centre Archives. http://circ.jmellon.com/docs/pdf/canadas_access_to_information_act_and_the_canadian_security_and_intelligence_community.pdf.
- Whitaker, Reg. 2015. The Failure of Official Accountability and the Rise of Guerrilla Accountability. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 205–224. Ottawa, CA: University of Ottawa Press.
- White, Ralph K. 1971. Propaganda: Morally Questionable and Morally Unquestionable Techniques. *The Annals of the American Academy of Political and Social Science* 398: 26–35.
- Zimonjic, Peter. 2016a. CSIS Using New Powers to Disrupt Terrorists since Bill C-51 Became Law. *CBC News*, February 23. <https://www.cbc.ca/news/politics/c51-law-disrupt-power-1.3460613> [accessed January 9, 2019].
- . 2016b. CSIS Head Says New Powers to Disrupt Plots Used Almost 2 Dozen Times. *CBC News*, March 7. <https://www.cbc.ca/news/politics/csis-power-disrupt-refugees-1.3479844> [accessed January 9, 2019].

Bills, Legislation, and Government Reports

- Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts*, 2d sess., 41st Parliament, SC 2015. https://www.parl.ca/Content/Bills/412/Government/C-44/C-44_4/C-44_4.PDF.
- Bill C-51, *An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, 2d sess., 41st Parliament, SC 2015. https://www.parl.ca/Content/Bills/412/Government/C-51/C-51_4/C-51_4.PDF.
- Bill C-59, *An Act respecting national security matters*, 1st sess., 42nd Parliament, SC 2019. https://www.parl.ca/Content/Bills/421/Government/C-59/C-59_4/C-59_4.PDF.
- Canada (Attorney General) v. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 2007 3 F.C.R.
- Canada. Parliament. House of Commons. 2016. Standing Committee on Public Safety and National Security (SECU). *Evidence of Proceedings*. 1st session, 42nd Parliament, Meeting 49.
- Canadian Security Intelligence Service. 1992. *1992 Public Report*. Government of Canada (Ottawa).
- . 2006a. Access to Information Act Request A-2017-37.
- . 2006b. *Public Report 2004-2005*. Government of Canada (Ottawa: Public Works and Government Services Canada). <http://publications.gc.ca/collections/Collection/PS71-2004E.pdf>.
- . 2008. *Public Report 2007-2008*. Government of Canada (Ottawa: Public Works and Government Services Canada). http://publications.gc.ca/collections/collection_2010/sp-ps/PS71-2008-eng.pdf.
- . 2010a. Canadian Security Intelligence Service Operational Data Analysis Centre Privacy Impact Assessment. Access to Information Act Request A-2016-393.
- . 2010b. *Public Report 2009-2010*. Government of Canada (Ottawa: Public Works and Government Services Canada). http://publications.gc.ca/collections/collection_2010/sp-ps/PS71-2008-eng.pdf.
- . 2015. *Public Report 2013-2014*. Government of Canada (Ottawa: Public Works and Government Services Canada). https://www.canada.ca/content/dam/csis-scrs/documents/publications/2013-2014_Public_Report_Inside_ENG.pdf.
- . 2015/2016. *ODAC Analysis & Investigations*. Access to Information Act Request A-2016-256.
- . 2016a. Access to Information Act Request A-2016-386.
- . 2016b. Launch of CSIS Twitter Account, <https://www.canada.ca/en/public-safety-canada/news/2016/07/launch-of-csis-twitter-account.html>.
- . 2016c. *Public Report 2014-2016*. Government of Canada (Ottawa: Public Works and Government Services Canada). <https://www.canada.ca/en/security-intelligence-service/corporate/publications/public-report-2014-2016.html>.
- . 2019. Mandate. Government of Canada (Ottawa). <https://www.canada.ca/en/security-intelligence-service/corporate/mandate.html>.
- Office of the Privacy Commissioner. 2014. *Special Report to Parliament: Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance*. Parliament of Canada, Government of Canada (Ottawa). http://publications.gc.ca/collections/collection_2014/priv/IP54-55-2014-eng.pdf.
- Privy Council Office. 2004. *Securing an Open Society: Canada's National Security Policy*. National Library of Canada, Government of Canada (Ottawa).
- Security Intelligence Review Committee. 2004. *SIRC Report 2003-2004: An Operational Review of the Canadian Security Intelligence Service*. Government of Canada (Ottawa: Public Works and Government Services Canada).
- . 2007. *SIRC Annual Report 2006-2007: An Operational Review of the Canadian Security Intelligence Service*. Government of Canada (Ottawa: Public Works and Government Services Canada).
- . 2015. *Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review*. Government of Canada (Ottawa: Public Works and Government Services Canada).
- X(re)*, 2013 FC 1275 (November 22).
- X(re)*, 2016 FC 1105 (October 4).

Appendix 1: CSIS's Definitions of "Associated Data"

- a. CSIS Director Michel Coulombe's statement during a Standing Committee on Public Safety and National Security proceeding (Canada 2016: 10): "Associated data is the context, not the content, of a communication. Such data is used by computer systems to identify, describe, manage, or route communications across a network. On its own, it does not identify individuals who are party to a communication."
- b. Internal CSIS PowerPoint presentation dated April 11, 2016 obtained through ATIA request: "Associated data is information, in structured fields, linked with a communication. Examples include email addresses, telephone numbers [redacted] as well as duration, dates and times of phone calls or Internet sessions. It does not include any information that could reveal the purpose of the communication, nor any part of its content."
- c. CSIS Assistant Director, Operations Enablement, John Cousineau's statement during a Standing Committee on Public Safety and National Security proceeding:

Associated data is data about a communication. It defines not the content of the communication, but it defines the communication event. The purpose of associated data is to help the network route to the information through the network. A very simple example would be that associated data would be a phone number, so the number that is called. Well, the reason that associated data is there is to actually route the telephone conversation to the right destination. That is what we were trying to explain when we said that associated data is used by the network to actually deliver information. Again, to reiterate, associated data does not describe the content of the communication. It simply describes the context. Classic examples would be date, time, duration, phone number dialed, etc. (Canada 2016: 13)

Appendix 2: CSIS's Definitions of "Metadata" (2005–2016)

- a. A 2010 document obtained through ATIA request titled "Canadian Security Intelligence Service Operational Data Analysis Centre Privacy Impact Assessment": "Structured information that describes the data; allowing management, control and understanding of other Information."
- b. A 2010 document obtained through ATIA request titled "Canadian Security Intelligence Service Operational Data analysis Centre Privacy Impact Assessment": "ODAC uses only metadata - data describing data - in its process. Metadata provides information about a data record that ODAC analysts exploit using information technology systems and applications, but it does not contain the actual business content."
- c. A July 20, 2006 letter from then CSIS Director Jim Judd to the Minister of Public Safety and Emergency Preparedness Stockwell Day, obtained through ATIA request: "In layman's terms, metadata is information that describes how, when and where a communication occurred."
- d. A 2015/2016 internal CSIS PowerPoint presentation titled "ODAC Analysis & Investigations" obtained via ATI request: "Metadata (or data about data) related to communications events. The best way to think of metadata is to think of a mail envelope with a letter inside; the letter is the content of the mail, but the mailing address, the postal stamp and the return address are the metadata, as they describe the activities of the envelope."
- e. SIRC 2014–2015 annual report:

Accordingly, it chose to define the parameters of its review using CSIS's own definition of metadata, which is "information collected via section 21 warrant that is associated with a communications event in order to identify, describe, manage or route that communication event or the means of its transmission, but excludes any information which could reveal the purport of the communications event, or the whole or any part of its content." (Security Intelligence Review Committee 2015: 24)