UNIVERSITY OF BRITISH COLUMBIA
SCHOOL OF PUBLIC POLICY AND GLOBAL AFFAIRS

Data Management and Bias Mitigation in the National Security Context

Prepared for the Canadian Security Intelligence Service

Melissa Hollobon
David Markwei
Claire Okatch
Savannah Tuck

TABLE OF CONTENTS

ABOUT THIS REPORT

This research project was conducted as a component of the Master of Public Policy and Global Affairs program (MPPGA) at the University of British Columbia (UBC). This research was supervised by Dr. Timothy Cheek, Dr. Julian Dierkes, and Corrin Bulmer of the UBC School of Public Policy and Global Affairs.

We would like to acknowledge the Canadian Security Intelligence Service (CSIS), the Academic Outreach & Stakeholder Engagement (AOSE) program, and the support received from Policy and Foreign Relations (PFR), for partnering with the School of Public Policy & Global Affairs for this project.

We extend our gratitude to all interviewee participants who provided their valuable time and insights for this project. We would also like to thank Dr. Julian Dierkes, Corrin Bulmer, and Dr. Timothy Cheek for their support and guidance.

We would like to acknowledge that this research project was conducted on the traditional, ancestral, and unceded territory of the xwməθkwəy̓ əm (Musqueam), Skwxwú7mesh-ulh (Squamish), and səl̓ilwətaʔɬ təməxʷ (Tsleil-Waututh) People.

AUTHORS

The student team who worked on this research project is comprised of four students who are currently undertaking the MPPGA program at UBC. Their biographies are as follows:

Melissa Hollobon

Melissa obtained a Bachelor of Arts in History and a minor in International Relations in 2018 from the University of British Columbia. During her undergraduate degree, she also completed the Hispanic and European Studies Program at the Universitat Pompeu Fabra. After graduation, she interned at the United Nations Environment Programme with the Convention on Migratory Species and with the British Columbia Council for International Cooperation as a mapping data analyst. She currently holds a position with the Dallaire Centre of Excellence for Peace and Security as a student policy analyst. In this position, her research is focused on the areas of human security and global governance, including the implementation of the Vancouver Principles and the advancement of the Women, Peace, and Security Agenda. In this research project, she hopes to utilize her previous experiences to address how bias in data contributes to inequities.

View LinkedIn

David Markwei

David earned a Bachelor of Arts in International Relations at the University of British Columbia in 2016 and is currently studying issues of development and social change within UBC's MPPGA program. Professionally, his work has involved coordinating projects with criminal justice professionals and legal researchers on various policy issues such as strengthening the protective environments in indigenous communities for children of parents in conflict with the law as well as access to justice for women living in rural and remote areas in British Columbia. He plans to use his experience developed from prior work related to issues in criminal justice and security policy, as well as the impact of institutional practices on marginalized communities to inform his contributions to this research project.

View LinkedIn

Savannah Tuck

Savannah holds a Bachelor of Commerce in Organizational Behaviour and Human Resources and a Diploma in Peace and Conflict Studies. The interdisciplinary field of Peace and Conflict studies reinforced Savannah's desire to address problems of human conflict and achieve justice through non-violent and constructive means that promote sustainability across social, economic, and environmental factors. Justice and equality are the driving principles around which Savannah plans to build her career. Savannah's previous experience and interest in the multidimensional aspects of security bring a unique perspective to the equity challenges arising around ethics and bias in data management practices.

View LinkedIn

Claire Louise Okatch

Claire Louise holds a Bachelor of Arts in Social Research and Public Policy and a minor in Mandarin Chinese from New York University Abu Dhabi (NYUAD). Within this degree, she specifically pursued ways in which policymaking can be more responsive to create space for the female, youth, and black voice. Since then, she has been involved in several grassroots initiatives in various parts of East and Southern Africa, the Middle East, as well as globally to this end by conducting both primary research and consultations with community groups. Most recently, she has co-authored a Gender+ Research Guide aimed at mainstreaming a Gender+ lens in research processes. She aims to bring her collective experiences to this project by centering marginalized communities who may be harmed by the insufficient considerations within security intelligence methods and practices.

View LinkedIn

CLIENT DESCRIPTION

DATA GOVERNANCE WITHIN THE CANADIAN SECURITY INTELLIGENCE SERVICE

As defined in section 2 of the *Canadian Security Intelligence Service Act* (CSIS Act, 1984), CSIS is tasked with investigating activities that are suspected of constituting threats to the security of Canada. CSIS is authorized to investigate threats of terrorism, espionage and sabotage, and foreign-influenced activities detrimental to the interests of Canada. Their core mandate consists of three pillars:

1. Investigating activities suspected of constituting threats to the security of Canada;
2. Advising the Government of Canada of these threats; and
3. Taking lawful measures to reduce threats to the security of Canada.

The *CSIS Act* of 1984, provides the legislative framework for the creation of CSIS. The Act mandates the gathering of information on those suspected of issues of national security such as espionage, political violence, and terrorism (Canadian Security Intelligence Service, 2020). More recently, the *National Security Act* of 2017 provided for the creation of the Office of the Intelligence Commissioner and the National Security and Intelligence Review Agency (NSIRA), which replaced a prior review agency, and added broader scope to review national security and intelligence activities across all federal departments and agencies.

Over the past couple of years, CSIS has recognized that certain intelligence collection and investigative techniques may perpetuate existing equity gaps and may disproportionately impact marginalized individuals. It is from this recognition that this project was created to evaluate and seek out best practices both from within CSIS and from outside the Service to ensure it fulfills its mandate in a manner that respects the *Canadian Charter of Rights and Freedoms*.

Our primary liaisons were representatives from the AOSE program, which acts as a bridge to link CSIS to Canadians. AOSE engages with stakeholders and thought leaders on national security issues and priorities to inform evidence-based decision-making and policy development.

The AOSE program aims to create a multi-disciplinary space within the Service to gain a deeper understanding of national security issues, drawing on a range of backgrounds and experiences to challenge assumptions and cultural biases, to enhance CSIS' research and analytical capacities.

OPPORTUNITY STATEMENT

The national security community recognizes the need to identify and integrate best practices to ensure that the analytical tools and methods used to manage data mitigate the perpetuation of bias and are accountable within a democratic context.

RESEARCH QUESTIONS

What are the forms of bias that could affect data management, and what could be the implications in the national security context?

Which groups could be disproportionately impacted by those forms of bias, and how do they experience this bias?

What are the existing best practices to address bias in data management?

How can the seemingly competing priorities of national security and the protection of personal freedoms be balanced, and lessons be learned from other contexts?

EXECUTIVE SUMMARY

With the emergence of big data, and new and emerging technologies and analytical tools for data management, security and intelligence agencies are rethinking the impact of bias in data management practices and how to fulfill this within their mandate. This represents a key dilemma on how to balance the need to ensure public safety while maintaining accountability in a democratic context. It is thus critical to identify best practices to ensure data management is free of bias and accountable within a democratic context.

This report is the result of a study involving stakeholders across federal government agencies, community organizers, civil society actors, and academics that aimed to explore this dilemma within the national security context. Our research set out to address four key questions:

1. What are the forms of bias that could affect data management, and what could be the implications in the national security context?
2. Which groups could be disproportionately impacted by those forms of bias, and how do they experience this bias?
3. What are the existing best practices to address bias in data management?
4. How can the seemingly competing priorities of national security and the protection of personal freedoms be balanced, and lessons be learned from other contexts?

Overall, our main takeaway is that **it is useful for CSIS to think of themselves as part of a broader federal ecosystem that is working to overcome systemic issues that may cause harm to certain groups** when either seeking service or protection from the government or may prevent them from doing so. By shifting this mindset, CSIS reaffirms its mandate to ensure a safe Canada, and allows for engagement with other departments to leverage existing practices, while adapting them to fit within the national security context.

More expansively, three key themes emerged from our research. The first theme revolves around **accountability and transparency**, which we divided into internal and external accountability. In this section, we highlighted how legal mechanisms such as the *CSIS Act* and the *Privacy Act* currently frames accountability actions by CSIS.

However, there exists an opportunity to expand this by showing an understanding of endemic data bias issues and involving stakeholders outside of CSIS working on these issues to build external accountability measures.

The second theme revolves around **anti-bias training and learning processes**, with a specific focus on culture change and digital literacy. Our research revealed that training on the topics of bias and digital literacy are critical components of best practices for ethical data management. As such, we recommend that the Service adopt an expanded definition of digital literacy that includes ethical considerations and an understanding of anti-bias frameworks, in addition to the necessary technical skills.

Our third theme encompasses **interoperability**; the ability of systems to exchange and use information. Multiple respondents cited an increased need for interoperability and cross-departmental collaboration on the issues of bias and data management. Our research uncovered four other agencies within the Government where CSIS can draw lessons: Statistics Canada, the Treasury Board Secretariat of Canada (TBS), the Standards Council of Canada, and other stakeholders operating under the Public Safety Canada portfolio.

In summary, our policy recommendations are as follows:

- Build on existing accountability mechanisms by engaging marginalized community voices both internally and externally.
- Bolster internal learning opportunities to incorporate digital literacy with awareness of endemic data bias issues to shift organizational culture.
- Increase interoperability by improving avenues for information-sharing on standards for good data governance and bias mitigation.

INTRODUCTION

Interlinkages Between Data, Privacy, and National Security

The world has increasingly been confronted with challenges that have called for more data. Key among them include the COVID-19 pandemic and an ever-evolving national security threat landscape. The onset of the COVID-19 pandemic and the unprecedented need for public health agencies to understand how the virus was spreading generated debate around privacy concerns and the collection and sharing of personal data. In Canada, initiatives such as the COVID-19 Self-Assessment Tool developed by Thrive Health and Health Canada demonstrate a partnership between public and private entities that developed data collection tools. This platform, and others like it, raised questions over regulatory and privacy protections given the separate accountability obligations that govern the use of data by public and private organizations. Additional public health measures to mitigate the spread of COVID-19 such as the performance of contact tracing raised further challenges over how to balance the need for privacy with the responsibility to protect the public good.

Like public health agencies, national security intelligence agencies have adopted data-driven tools to improve efficiency and organizational capabilities. Reliance on bad or biased data can lead to bad or biased results and decisions. However, it is important to consider the interdependence of data and analytics. Data only becomes meaningful once it has been processed and analyzed, and context is considered when analyzing data. Yet, the tools and analytical methods used to analyze data can reflect biases that could lead to disproportionate impacts on certain groups.

To understand CSIS' positionality with data bias and data governance, it is important, to begin with the *CSIS Act* of 1984, from which the organization derives its mandate. For example, sections 11.01 to 11.25 of the *CSIS Act* establish the need for judicial authorization for the retention of a Canadian dataset by the Service and Ministerial authorization for the retention of a foreign dataset. This requirement places a specific onus on CSIS to maintain good practices regarding its data collection methods, to ensure collection methods are limiting intrusion into the private lives of Canadians, and collection is only undertaken if the data is relevant to the performance of the Service's duties and functions, as highlighted from sections 12 to 16 of the *CSIS Act*.

On the other hand, section 12 of the *CSIS Act* enshrines the principle of "strictly necessary" as it relates to the collection of information and intelligence if there are reasonable grounds to suspect any threat to the security of Canada. This responsibility raises concerns over how to deal with accountability in a context that is fast-paced, relies on incomplete information, and has consequential impacts. As discussed again later in this report, government-wide initiatives have adapted to this increased need for accountability. This includes TBS' Algorithmic Impact Assessment (AIA) or the implementation of Gender-Based Analysis Plus (GBA+) across federal departments and agencies. However, the shift towards information both from and about threat actors being increasingly available online in digital forms, demands a re-examination of current strategies.

The Current Context: Why is this Important for CSIS to Think About Now?

Since the beginning of the post-9/11 period, a major policy focus of national security organizations continues to be placed squarely on how to anticipate and intercept potential terrorist threats. Furthermore, the killing of George Floyd by Minneapolis police officer Derek Chauvin in Minnesota in 2020 marked a tipping point, spurring the conversation to reform the governance practices of public agencies to reduce both the prevalence of bias and disproportionate harm to communities of colour. This was also joined by broad calls for a commitment to better incorporate principles of intersectionality, equity, and inclusion into the work and structure of Canada's federal public service, including the country's national security sector. For example, in January 2021, the Clerk of the Privy Council and Secretary to the Cabinet released a Call to Action on Anti-Racism, Equity, and Inclusion in the Federal Public Service, a public-facing document that reflected on the "unjust treatment of Black people, other racialized groups, and Indigenous peoples…" and challenged the public service leaders to implement several inclusive reforms and to create more opportunities for Black, Indigenous, and other racialized communities within their departments. These calls recognized that structural bias in the institutional foundations that support national security activities inevitably can lead to bias in program delivery.

In line with these larger conversations, CSIS is also taking steps to expand its understanding of bias and better incorporate principles of diversity, equity, and inclusion. For example, there is currently an internal Black, Indigenous, and People of Colour (BIPOC) network that works with the Service's Director to help improve understanding of the experiences of racialized employees. Additionally, there exists a Women in Technology focus group that encourages women within CSIS to join directorates working in data-focused areas. Initiatives like this emerged from Government of Canada public servant associations and networks. Furthermore, innovative technology is in development internally to support employees to incorporate GBA+ into their work by presenting decision-making points that identify assumptions and potential biases. These steps are indicative of the precautionary principle, which advocates for more robust thought on the implications of technological innovations and methods because of their potential for harm. When this principle is applied in this context, it frames these steps as a proactive measure in understanding the effects of bias and taking active steps to mitigate it.

The analysis in this report builds on the work CSIS has been involved in with the National Security Transparency Advisory Group and the establishment of divisions such as the AOSE program. Based on the analysis, this report provides recommendations on how to integrate good data governance approaches within the Canadian national security context, to mitigate the perpetuation of bias in data, while increasing transparency, accountability, and a duty of candour to Canadians.

METHODOLOGY

The research methodology consisted of a secondary literature review, semi-structured interviews, and thematic analysis. The secondary literature review revealed trends and issues regarding the collection and use of data within the national security sector and related contexts, including the disproportionate impacts and risks to various communities due to underlying biases that inform data management processes. Further, the literature provided case studies that highlight bias-driven impacts on communities from the use of data by intelligence agencies in democratic contexts, as well as best practices that mitigate bias, strengthen accountability mechanisms, address ethical challenges, and improve public trust in the handling of data by government organizations. We compiled and reviewed several resources from academia, government, and civil society sectors and will incorporate relevant findings within our analysis in subsequent sections.

We conducted 16 semi-structured interviews with participants from academia, community organizations, and various Government of Canada departments. Interviews occurred virtually for no more than 60 minutes and our project team rotated between four roles during each session: a primary interviewer, a secondary interviewer, and two notetakers.

Following our interview period, we analyzed our findings through a thematic analysis process in which we reviewed our fieldwork notes in stages. In the first stage, we annotated each of the notes with our initial observations, interpretations, and insights. In the second stage, we began to identify patterns within the notes and group them into high-level themes. In subsequent stages, we further refined those themes and synthesized our findings. These themes have been incorporated into the analysis within our report, and highlight key challenges, impacts, opportunities, and best practices relevant to the issue of bias within data management in national security organizations.

Throughout our research process, we used the following framework of analysis:

Policy Forward Versus Policy Endemic Lens

In our approach to our research questions, we distinguished between larger structural issues affecting data management practices and influencing data bias, and those issues that could be deemed more current or salient. This distinction is explained by the terms policy forward and policy endemic. Policy forward refers to issues within the national security context that are deemed to be the more pressing issues relating to the threat landscape. On the other hand, policy endemic refers to the longer-term, systemic issues that are apparent in the national security context, but also extend to society as a whole. Using this terminology allows us to better understand the root causes of the issues around bias in data management, and to provide CSIS with actionable recommendations and a holistic understanding of the issues of bias in data management in the national security context.

FINDINGS, ANALYSIS, AND RECOMMENDATIONS

Definitions of Bias and Identification of Impacted Groups

“The thing about intelligence agencies is that they are in the business of bias. The very idea that you have to study characteristics and pre-empt what may put people in harm’s way is an exercise in some form of bias.”

These words from one of our interviewees encapsulate what makes this question of bias a tricky subject to solve. This interviewee reframes intelligence work as an exercise in drawing out patterns and seeing their repeated occurrence as a form of bias. This implication raises questions over whether intelligence work can ever be free of bias if the very nature of it is to be biased in order to pre-empt harm. As we heard from multiple sources, complete elimination of bias in data may not even be possible. Instead, emphasis has been on how we can re-examine data management practices to understand how they cause harm, to whom this harm is caused, and learn how to further mitigate the impacts. Developing a holistic understanding of how bias is present within data management and employing governance practices that effectively mitigate its incidence must involve identifying where exactly bias occurs along with the upstream and downstream processes involved in the life cycle of data. To answer these questions, we interviewed a broad array of actors who have knowledge of data bias both from a design and experiential perspective. Our logic was to begin our analysis beyond a textbook version of data management bias, prompted by the work of Dr. Sasha Chock of Design Justice, who points out that where these questions are asked has a significant impact on the kinds of responses that we eventually get.

What is data bias?

Data bias can be defined as the ways in which subjective assumptions regarding race, gender, and other social groups are embedded within the collection and application of data. Data bias can occur at both the individual and institutional levels. In terms of individuals, people who work with data may for example possess stereotypical assumptions about various groups that inform how they interact with data. At the institutional level, agencies and organizations are often at risk of reflecting social biases within their data policies and practices. Data management as a term encompasses separate tasks each of which raises novel issues surrounding how bias occurs within the use of data by public agencies, as well as the consequent risk of harm to marginalized communities. We can thus see how data bias can perpetuate structural inequalities against historically marginalized groups when it is present at both the individual and institutional levels.

There is a commonly held belief that data is neutral and objective. However, this notion has shifted to recognize that data needs to be understood within a certain context, and that data is subject to biases. From the literature, bias in data can be defined in two ways. First, drawing from statistics, bias can arise from any systematic difference between true parameters and samples. Bias in data emerges from inaccurate representations of a population or study, this can include data that does not include variables that inaccurately capture the predicted phenomenon or data produced by humans which may contain bias against groups of people (Lopez, 2021). Both can result in unintended impacts and harms. One interviewee described bias as “basically a difference in treatment in individuals or situations, groups or areas, based on differing characteristics.”

Consequences of Data Bias

One interviewee raised the importance of equipping national security personnel with information on how biased information can impact their conclusions. For example, one interviewee stated that “before 2013/2014, women were not considered when analyzing terrorist or ideologically motivated threats.”

One way bias in data management manifests in the national security context is the excessive policing of some groups over others. Under Canada’s Passenger Protect Program, an air security program that prevents individuals who pose a potential threat to air security from boarding a plane (Government of Canada, 2021), it is estimated that more than 100,000 Canadians have the potential to be adversely affected from false-positive screenings because of similar names (No Fly List Kids, 2017). This number reflects a substantial number of individuals who may be subject to unintended harm.

Law enforcement and security agencies in Western democratic contexts have a well-documented history of causing disproportionate harm to marginalized communities and people of colour through practices such as excessive surveillance, detainment, and violations of constitutional rights. While there has been some progress toward more equitable, progressive practices, such groups still face a disproportionate risk of harm due to persistent structural discrimination and historical biases deeply embedded within the institutional systems of public safety and security agencies.

With regards to racial or ethnicity-related bias, for example, a commonly shared sentiment from our interviews was that Black and Brown communities often experience greater levels of targeting by law enforcement and security agencies due to assumptions about their involvement in crime or terror-related activities. This leads to their over-representation in databases and datasets that subsequently inform the deployment of data-driven tools and methods aimed at predicting future crimes or acts of terror. In Canada, Black, Indigenous, and other racialized communities are more likely to experience racial profiling and questioning by police officers. They are also more likely to be added to databases regarding suspected gang affiliations or as persons of interest, which in turn arbitrarily increases their likelihood of arrest or detainment in connection with suspected criminal activity (Robertson, Khoo, and Song, 2020). In other democratic contexts such as the United Kingdom, expanded anti-terrorism legislation following the 9/11 and 7/7 attacks led to increased surveillance and intelligence gathering on British Muslims and South Asians, further reinforcing systems of discrimination, marginalization, and victimization against their communities (Mythen, Walklate, and Khan, 2009). These trends are harmful to racialized groups as they institutionalize negative perceptions regarding their communities. As one interview participant noted, the more police and security agencies target such communities, the more they are put at risk of being viewed as inherently nefarious and suspicious, thus further marginalizing them.

Biased data is also understood among community groups who identified as persons of colour as having implications for their access to resources. For example, in British Columbia (BC), there was insufficient monetary support for the Black community to offset the effects of the pandemic. Looking at marginalized groups such as Blackness as a monolith creates issues for effective service delivery. Within each marginalized group, there could be further marginalization across other identity indicators such as able-bodiedness, sexual orientation, or single-parenthood. The gaps in disaggregated data collection, as evident in this specific example, demonstrate how gaps in (disaggregated) data collection create systemic erasure. This marginalization points to a policy endemic issue of systemic, disproportionate resource allocation for communities of colour.

DATA LIFE CYCLE

It is critical to uncover how bias intrudes into data management practices and what the consequences of this intrusion are in the national security context. Using a data lifecycle approach allows us to map out at what points bias is intruding and understand that these technologies are an end, whose use is informed by certain biases and assumptions.

Stage	Definition	Risk	Examples
Planning	Decision-making to inform the collection and operationalization of data.	Lack of consultation with external communities at this stage increases the risk of perpetuating harmful outcomes at downstream stages due to the exclusion of perspectives to counter internal biases within organizations/leadership.	Black, Indigenous, South Asian and other communities that have historically been unfairly targeted by data-driven technologies often report a lack of awareness or consent to their data being collected by security/intelligence agencies.
Collection	Gathering and measuring information on variables of interest in a systematic fashion to evaluate/predict outcomes.	The methods used to collect data (social media scanning, facial recognition, biometrics, etc) can be impacted by bias that leads to the overrepresentation or underrepresentation of various groups in databases.	The deployment of surveillance technology by security agencies is not often evenly distributed, as it favours non-White communities that are perceived as likely to harbor threats. Non-White communities are also more likely to experience practices such as carding as part of intelligence gathering by police departments. This leads to those communities being overpoliced/securitized.

Processing	The process of manipulating data from its raw from into usable information.	Bias at this stage can lead to inaccurate interpretation/representation of data collected from communities that enables harmful action against those communities when the data is operationalized.	The annotation of raw data is often influenced by stereotypical correlations and social biases in terms of race, gender, etc. For example, information collected from Black/Brown communities is more likely to be correlated with gang/terrorist activity.
Analysis	Generating insights from data and using findings to inform policy.	Individual or institutional bias can lead to subjective interpretations of data against various social groups and result in disproportionate harm or the exacerbation of inequalities.	When government and security agencies develop national security or crime policy, they often target non-White communities based on subjective information that these communities are more likely to engage in criminal behaviour (for example drug enforcement policies, immigration restrictions, etc.)
Application	The operationalization of data in advanced technologies or other applications.	Technologies that are trained with biased data can cause harm against communities when they are applied in the field.	Biometric scanning and facial recognition technology in airports have been shown to flag travellers from non-White communities as potential risks.
Retention	The protocol within an organization for storing data for a specified period for operational or regulatory compliance needs.	The longer data is stored, the more likely it is to be exposed to data breaches and also re-used in applications that go beyond the original purpose behind the collection of that data. This particularly impacts marginalized communities that share data with government agencies without knowledge of how their data may be shared internally and repurposed.	Institutions and agencies have often collected data from marginalized communities without proper transparency around how long their data will be held and who will have access to it. This has led to violations of community privacy and harm to communities for example when sensitive data is made public through freedom of information (FOI) requests.

ACCOUNTABILITY

The Role of Accountability Within Data Management: Internal and External Dimensions

A key theme from our research and fieldwork interviews was the importance of accountability in governing the collection and use of data by intelligence agencies. Accountability with data management applies both internally within the structure of an organization and externally in terms of the various obligations of that organization to members of the public whose personal data it collects. Accountability also encompasses transparency in terms of how organizations disclose information about the data they collect, the way they operationalize data, and the impacts generated by their use of data. Strong accountability measures contribute positively to mitigating the presence of bias and risks of harm from the collection and use of data. They do so by helping prevent the exploitation of data, refining the quality of data, and incentivizing careful consideration of potential risks or harmful impacts from data-driven decisions. By mitigating these issues, good standards of accountability and transparency also have a value-added benefit of strengthening public trust in the ability of government agencies to handle data responsibly, ethically, and with adherence to democratic principles. Without good standards, citizens within democratic contexts are less likely to trust government agencies that hold their data because they neither understand nor feel consent to the decision-making processes that inform the collection and use of their data. This in turn leads the public to feel naturally suspicious or unsafe, particularly with agencies that engage in surveillance and have the potential to cause harm with their data (Parsons, 2020). In an interview our team conducted with an official from CSIS, the interviewee affirmed that it would be ideal for the Service to have a clear social contract with Canadians regarding how it collects personal/private data, the authorities which enable data collection to occur, as well as how data is kept or destroyed. This sentiment highlights positive will within the Service to be more accountable to Canadians by improving transparency around how it uses private data, thus improving public trust in the process.

There are good internal accountability practices within the Government of Canada that regulate the use of data by public agencies such as legislative controls (*Privacy Act*, *CSIS Act*, etc.), review agencies, and AIAs. However, policy endemic challenges include formalizing the level of risk assessment within security agencies such as CSIS to regulate the use of new and emerging technologies, as well as a lack of sufficient transparency with the public regarding the processes and protections that govern the use of data.

Building Public Accountability in Data Management: The Case of Estonia

The Government of Estonia can be considered as a model case that not only highlights the value of adopting strong, formalized internal accountability measures to govern the use of data but how good transparency and public engagement practices promote ethical data use and public trust in public agencies. In the wake of a series of cyber-attacks on the public information infrastructure, the government established the Estonian Information System Authority (EISA) to enforce common data security practices across government departments. These practices include the Estonian information security standard (E-ITS), a mandatory information security standard to ensure all government departments have a baseline data protection system (Republic of Estonia Information System Authority, 2022). The Estonian Government also made a concerted effort to be transparent with the public about the extent of the cyber-attacks on its information infrastructure and source feedback from citizens regarding measures to improve the security of their data. These combined efforts successfully improved the cohesion of internal accountability standards within the government, and improved trust by the people of Estonia in the government's data management and governance processes (Priisalu and Ottis, 2017).

Internal Accountability: Legal and Technical Frameworks

Internal accountability frameworks are essential for public agencies that work with data given the rapidly increasing sophistication of data that is collected and the proliferation of data-driven advanced technologies, tools, and methods. Such frameworks are particularly important for security organizations given the sensitive nature of the data they work with as well as the focus of their work on anticipating and intercepting emerging threats to the public and national security. From a policy endemic perspective, as data-driven technologies such as artificial intelligence (AI) and machine learning systems grow more complex, so does the risk of harmful outcomes from the use of such technologies. An interviewee from an academic think tank for example noted that the risk of poisoning datasets in the national security sector can impact the way defense systems managed by AI or machine learning systems are deployed. This could lead to dangerous outcomes particularly when those systems are released on a large scale. There is thus a continued need for security agencies to follow strong internal accountability measures that promote ethical, lawful, and responsible data management practices to prevent unintended harm.

Internal accountability with regards to data management by national security agencies usually involves the use of legal and technical tools to regulate factors such as how much data these agencies can collect, the type of data they can collect, the sources they collect their data from, and potential risks from the use of that data. The *CSIS Act* stipulates specific accountability obligations of the Service regarding its data practices, for example in the requirement of judicial authorization for retention of Canadian datasets (section 11.13) as well ensuring actions by the Service to respond to threats are “reasonable and proportional”, and do not cause unneeded harm to third parties or infringe on their right to privacy (section 12) (Justice Laws Website, 2022).

As the data collection capacity of security agencies such as CSIS continues to expand through the use of emerging technologies, it will be useful to continue to consider policy endemic issues such as how to ensure respect for the privacy of communities within Canada. This for example involves the question of how to maintain adherence to existing legal protections granted to members of the public regarding their right to privacy. The *Privacy Act* obliges government agencies to respect the individual privacy of Canadians by, for example preventing the indiscriminate collection of personal information. The Privacy Commissioner, a position appointed by the Parliament, also acts to advocate for the privacy of Canadians as enshrined within the *Privacy Act* (Office of the Privacy Commissioner, 2015).

Another avenue of internal accountability with regards to the use of data by Canada's national security agencies exists through the responsibilities of the National Security and Intelligence Review Agency (NSIRA). NSIRA possesses a mandate to inspect the activities of CSIS, the Communications Security Establishment (CSE), and the national security and intelligence work of all other federal departments and agencies. To enable the exercise of its duties, NSIRA possesses unrestricted access to classified information controlled by the agencies it reviews. The statutory powers granted to NSIRA come from the *NSIRA Act*, which enables the agency to access information freely and conduct reviews independently (NSIRA, n.d.). NSIRA has conducted various reviews of CSIS regarding aspects such as the Service's threat reduction activities, its relationship with police departments during investigations, as well as the work of the CSIS Internal Security Branch. In 2019, NSIRA released findings from a review of the Service's use of geolocation data and noted a risk regarding the potential breach of section 8 of the Charter concerning protections against unreasonable search and seizure (NSIRA, 2019). To mitigate this risk, NSIRA recommended the provision of continuing legal support through the Department of Justice to ensure that any use of technology by security agencies for applications such as the collection of geolocation data is legal. Another recommendation within the report is for the development of policy to incorporate risk assessments "when information collected through new and emerging technologies may contain information in respect of which there may be a reasonable expectation of privacy" (NSIRA, 2019, p.16).

The Government of Canada also mandates the use of an AIA in the use of automated decision systems by government agencies. AIAs help public agencies perform risk assessments to determine potential short- and long-term impacts from the deployment of automated systems. They can be particularly useful for identifying and mitigating bias within data management processes by providing a framework for agencies to evaluate the risk of harmful outcomes from the collection and use of data belonging to different communities (Reisman et. al, 2018). A key element within AIAs is the requirement for third-party review via consultation with public stakeholders to generate feedback on the design and purpose of automated systems. The Canadian government's AIA tool, facilitated by TBS, provides questions around aspects such as the risk profile, decision-making, and nature of data used within an automated system (Government of Canada, 2021). In an interview with a representative from the Treasury Board, the participant mentioned that a key limitation of the AIA is that its scope only currently applies to administrative decision-making within government, therefore cannot cover use cases such as the collection of data by agencies such as CSIS or the use of AI to inform policy. However, their department remains prepared to provide technical and funding support to government departments that wish to incorporate impact assessments in their work.

External Accountability: Transparency, External Review, and Building Public Trust

External accountability measures regarding the management of data by public agencies encompass transparency over how personal/private data may be collected, used, and protected. Transparency can also involve accommodations for the public to consent to the use of their data, as well as feedback loops for stakeholders to provide input on the internal data management processes used by public agencies. These factors collectively contribute to fostering an environment of trust by the public in the use of personal data by government agencies. Regarding the issue of consent, the Office of the Privacy Commissioner (OPC) has stated that “organizations are generally required to obtain meaningful consent for the collection, use, and disclosure of personal information” (Office of the Privacy Commissioner, 2021). The OPC has also provided principles to organizations regarding consent as reflected in legislation such as the *Personal Information and Electronic Documents Act* (*PIPEDA*). One of the key recommendations within these principles is for organizations to constantly be ready to demonstrate compliance with accountability measures such as consent standards in response to inquiries from regulators or the general public. The OPC also explains the importance of consent given the sensitivity and risks from the use of certain forms of personal information by organizations such as ethnic/racial origins, political opinions, genetic and biometric data, sexual orientation, and religious beliefs. Although the level of confidentiality CSIS requires in its work makes obtaining express consent difficult when collecting data, it can still be useful for the Service to consider how to extend agency to various communities regarding their data by engaging in public consultation processes and openly sharing information with the public on how their data is protected within the Service.

Measures that promote external review of data management processes, tools, and methods can also help reduce bias particularly when feedback is provided by diverse groups that are at greater risk of harm from the use of their data by public agencies. The national security sector is uniquely positioned in this conversation given the expectation of confidentiality within its work. However, a lack of sufficient transparency and engagement with diverse communities over the collection and use of data by intelligence agencies can erode the trust of the public in the ability of agencies to work with data in a responsible manner. In 2020, the OPC commissioned a survey of Canadians on privacy-related issues. Within the survey, 53% of Canadians disagreed that the Government should have powers to collect personal information as part of intelligence work. In addition, 59% of Canadians responded no to giving up some personal privacy to allow the Government to conduct intelligence work (Office of the Privacy Commissioner, 2020). These results highlight a considerable level of distrust by the public regarding the data practices of Canada's security agencies. Applying a policy forward lens to understand the results is also useful in this case because their implication is that for reasons of legitimacy, security agencies will need to invest more in building trust with Canadians as they continue to utilize more sophisticated methods to collect and use data to respond to evolving threats against Canada's national security.

An overemphasis on confidentiality, particularly when the underlying reasons are unclear, negatively impacts the relationship between security agencies and the communities they serve and protect. Interview participants noted that people presume the worst without sufficient information and that to hold back information due to privacy concerns or to release surface-level data without context only leaves room for more questions.

In addition to this, participants further noted that it would be constructive for national security agencies to be more open to review from external stakeholders, and for the results of those reviews to be shared in a summary format with the public rather than for such agencies to be exempted in a blanket fashion from various review processes. One interviewee for example suggested that instead of maintaining a total wall around their practices, national security organizations can instead explore "windows and doors for more transparency." This sentiment is shared by officials within CSIS, as interviewees from within the Service also mentioned that there is internal support for increasing transparency and sharing more information with the public to show how it uses data responsibly. At the same time, multiple interviewees did affirm that national security organizations such as CSIS need to maintain some level of confidentiality with regards to the data it collects to protect the privacy and safety of Canadians. However, an area of compromise could be for the Service to explore how it can be more transparent regarding the policies and processes that inform its collection and use of data.

> "Ultimately, we do need a wall between intelligence and society, but it can't be a total wall. We need windows and doors where conversations can take place."
>
> - Dr. Stephanie Carvin

A potential avenue that the Service can explore to strengthen transparency with its data policies and processes is to provide space for external stakeholders from diverse communities to audit internal data management systems, tools, and methods. To avoid potential risks such as privacy or confidentiality breaches, these audit channels can focus primarily on the upstream stages of data management such as the decision-making processes that determine how data is collected and used rather than the content of data. In our interviews, several participants both external and internal to CSIS expressed support for more third-party audits of the processes that underpin data collection within the Service to help improve the strength of its data governance system.

Promoting Public Engagement in Identifying Potential Harm by New Technologies: The Algorithmic Equity Toolkit

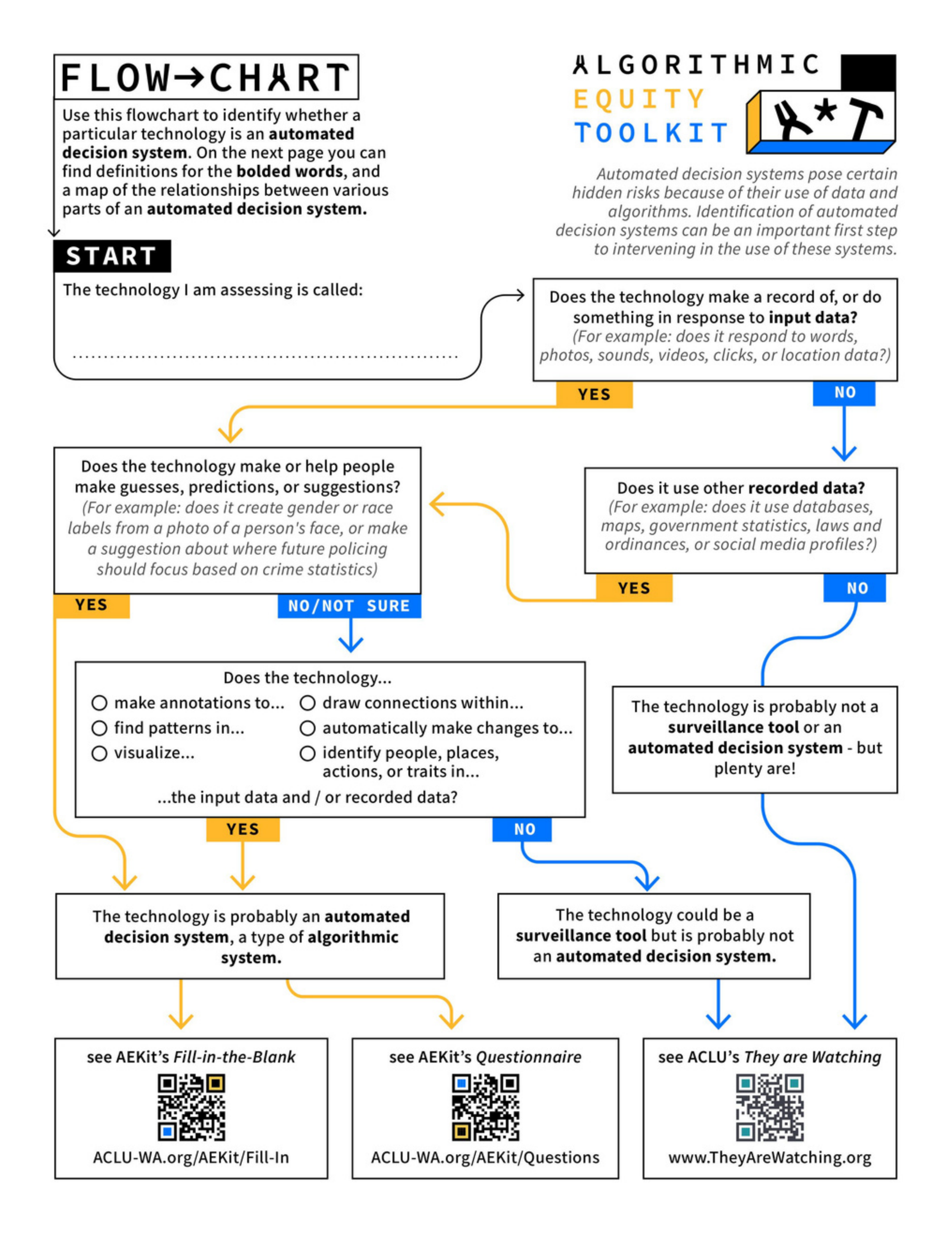
FLOW→CHART
Use this flowchart to identify whether a particular technology is an **automated decision system**. On the next page you can find definitions for the **bolded words**, and a map of the relationships between various parts of an **automated decision system.**
ALGORITHMIC EQUITY TOOLKIT
Automated decision systems pose certain hidden risks because of their use of data and algorithms. Identification of automated decision systems can be an important first step to intervening in the use of these systems.
START
The technology I am assessing is called:
Does the technology make a record of, or do something in response to **input data?** *(For example: does it respond to words, photos, sounds, videos, clicks, or location data?)*
YES
NO
Does the technology make or help people make guesses, predictions, or suggestions? *(For example: does it create gender or race labels from a photo of a person's face, or make a suggestion about where future policing should focus based on crime statistics)*
Does it use other **recorded data?** *(For example: does it use databases, maps, government statistics, laws and ordinances, or social media profiles?)*
YES
NO
YES
NO/NOT SURE
Does the technology...
○ make annotations to...
○ find patterns in...
○ visualize...
○ draw connections within...
○ automatically make changes to...
○ identify people, places, actions, or traits in...
...the input data and / or recorded data?
The technology is probably not a **surveillance tool** or an **automated decision system** - but plenty are!
YES
NO
The technology is probably an **automated decision system**, a type of **algorithmic system.**
The technology could be a **surveillance tool** but is probably not an **automated decision system.**
see AEKit's *Fill-in-the-Blank*
ACLU-WA.org/AEKit/Fill-In
see AEKit's *Questionnaire*
ACLU-WA.org/AEKit/Questions
see ACLU's *They are Watching*
www.TheyAreWatching.org

FIGURE 1. THE AEKIT FLOWCHART

In the United States, an Algorithmic Equity Toolkit was developed as part of a participatory design process involving stakeholders from organizations and academic institutions such as the American Civil Liberties Union of Washington, the Digital Life Initiative at Cornell University, and the School of Information at the University of Michigan. The toolkit provides a framework for community members to identify whether a particular technology relies on AI and to interrogate risks of algorithmic harm and bias within that system.

An added benefit of the toolkit is the flexibility within its design to encourage users to identify potential harms not only within technologies used by law enforcement or security agencies but also within other sectors such as transportation, housing, etc. (Krafft et. al, 2021). Adoption of tools such as the AEKit has the double-sided benefit of allowing communities to better protect themselves from potential harm by helping public agencies adopt data-driven technologies in a more ethical manner. Additionally, by incorporating this form of public engagement to inform their data management practices, government agencies can also strengthen their systems of transparency and external accountability as well as improve public trust.

SUMMARY OF RECOMMENDATIONS:

- Strengthen internal accountability obligations by implementing a holistic risk assessment process similar to the AIA tool to govern the collection and use of data particularly with new and emerging technologies.

- Strengthen external accountability and transparency by expanding public disclosure of information such as policies behind the collection of personal/private data by the Service, how the use of the data is regulated, and outcomes from the use of data.

- Explore avenues to incorporate greater audit of the processes behind the Service's use of data by diverse communities through consultations and frameworks such as the Algorithmic Equity Toolkit.

LEARNING PROCESSES

Culture Change and Digital Literacy

To mitigate bias in data management, it is important to develop an internal organizational culture that understands the impacts of bias on marginalized communities and integrates bias-mitigation practices into the development of digital literacy skills. Using the policy forward lens, we recognize that salient data management issues may bring stakeholders together or instigate new learning processes. However, if they are not rooted in an understanding of endemic issues, they are likely to be short-term and have comparatively less impact on organizational culture. Addressing these issues requires a longer-term approach. Furthermore, an understanding of endemic data bias issues enables organizations to be effective at recognizing policy windows for organizational change.

During fieldwork, we focused on methods of learning about bias, what channels exist to understand it, and what strategies exist to constantly work to mitigate it. In our understanding of this theme, we were cognizant of different definitions of bias. One example is that an interviewee preferred to use the term "performance differential" rather than bias because the latter emphasized human nature rather than the technical aspect. This desire to make a distinction between humans and technology implies a difference in understanding of who was responsible for data bias. As such, we found it important to further delve into how people developed their understanding of bias and how this connects to data management. We identified key avenues to promote understanding of bias and connected this to the current efforts of the Service to improve diversity, equity, and inclusion.

The following are three key avenues we identified:

The Resurgence of DEI Initiatives Due to Key Political Events

From our interviews with individuals from marginalized communities, questions over data bias were framed as a policy endemic issue and the 2020 reckoning was seen as a long-overdue wake-up call.

This long-term view would be valuable insight to harness in designing learning processes that address any data bias.

When analyzing the impact of 2020 through a policy forward lens, it underscores how the political saliency of this moment brought the marginalization faced by the Black community to the forefront. However, it is also concerning that it implied a beginning point for the conversations on racial bias in data as the communities we spoke to did not reference it as the start point. In Design Justice, Sasha Chock explores how narratives around social movements influence design processes noting that one of the "most powerful" outcomes of the interaction of these concepts is "how we frame the problem" (Constanza-Chock, 2020). Framing the 2020 racial reckoning as a current moment rather than an illustration of long-term endemic marginalization changes how we may view its importance. For example, if issues around marginalization are understood as endemic, this can encourage a deeper investigation into data management processes and bias mitigation.

When conducting interviews for this research, five participants out of the sixteen in total brought up either the 2020 racial reckoning or referenced George Floyd when referring to a shift within their department or workplace towards addressing the issues of equity and inclusion. For example, during an interview with a GBA+ instructor, they described how this trend was also apparent with gender-sensitive training since there was a resurgence of interest in GBA+ after 2020 even though it was already a government-mandated tool. Our assessment of this resurgence is that it provided a politically salient moment to re-examine how data bias reinforces marginalization. It is imperative that learning from marginalized communities on a long-term basis is part of the design of the data management process in the national security context.

Employee Networks and Leadership

The BIPOC and Women's Network within CSIS were both described by respondents as steps towards inclusion and support for marginalized groups within the service. The Women's Network was developed to inform on gendered issues, diversity, and career advice, and the BIPOC network has been meeting with the CSIS Director in small groups to discuss experiences of working within the Service (Tsalikis, 2020). Additionally, these networks also function as a source of community and support building.

Across departments, when government leaders met consistently with representatives of these employee networks, this was a positive indicator that key issues were receiving attention from leadership. Leaders play an important role in supporting anti-bias learning plans and initiatives both within CSIS and other federal agencies. An example would be the account that the ministers in government were a key focal point in the ask to re-examine how disaggregated data may help further understand the plight of marginalized communities. Additionally, leadership can influence employee learning pathways to emphasize understanding bias, marginalization, and data management. This can be achieved through Individual Learning Plans which include mandatory and optional training courses offered by the Government of Canada and are discussed between managers and employees.

Although leadership seemed to play a vital role both in resource allocation and prioritization of equity lenses, initiatives such as learning plans or diversified hiring approaches did not tell us much about how leadership was stepping up to the task of learning about endemic bias in data. For example, accountability on learning plans was always described as a discussion with a manager or a superior. Since leadership was implied to be crucial to how equity networks organize or how learning plans adapt, there is a need to pay particular attention to how internal leadership constantly keeps abreast of and adapts to the knowledge of data management bias to ensure they continue to create conducive environments for learning to occur.

Anti-Bias Training as a Component of Digital Literacy

The definition of digital literacy has remained complex and fluid, as the term continues to evolve as technological advances and global digitalization continues (Bejaković, & Mrnjavac, 2020). Rather than a set of hard skills, the definition of digital literacy repeatedly falls under the idea of competence and systems understanding in relation to technology and the digital world and how these systems function within legal and ethical constraints (Bejaković, & Mrnjavac, 2020). Therefore, digital literacy needs to be thought of in an expanded way, more towards systems thinking and competencies rather than only defined as hard technical skills. This expanded definition of digital literacy would therefore include anti-bias measures and DEI values.

A Holistic Approach to Digital Literacy

One framework for digital literacy is the Digital Competence Framework from the European Commission, which considers social well-being, privacy, and inclusion. Its five competencies are briefly stated below:

1. Information and data literacy
2. Communication and collaboration
3. Digital content creation
4. Safety
5. Problem-solving

The framework offers a more holistic approach to teaching digital literacy, as it brings in ethical considerations alongside the necessary technical skills. For example, the competency of "safety" refers to the protection of privacy, awareness of well-being, and social inclusion. Additionally, "problem-solving" refers both to competency around being constructive and reflective, traits that would assist with understanding downstream impacts of data that may not be immediately obvious. These principles are transferable to the Service as it aims to improve bias mitigation in relation to data management. Expanding digital literacy competencies has also been identified as a concern across the Government of Canada for the public service, and this will continue to be a topic of interest in the coming years (GoC, 2017).

Throughout the expert interviews, many participants also referenced the value of individual or departmental training on the topics of bias and digital literacy as crucial for their position. GBA+ was often referenced during interviews as a training policy that was important to create a standard of understanding amongst departments on how to incorporate a gendered lens throughout planning processes and decision-making.

The Canadian government has worked to mainstream GBA+ across all departments, programs, and planning processes at all levels (WGEC, 2021). The history of the framework draws on previous feminist foundations and in 2012 added the "plus" to encompass an intersectional lens (Christoffersen & Hankivsky, 2021). However, there is still a long way to go in making lessons from GBA+ mainstream and to fully incorporate the "plus" (an intersectional lens) in decision making processes (Christoffersen & Hankivsky, 2021).

Additionally, interviewees across departments were familiar with GBA+ but suggested that the incorporation of an intersectional framework was not as developed. For example, multiple identity factors would be analyzed in separate considerations and categories. We found evidence of this in the ways in which our interviewees discussed marginalization often making the distinction between initiatives on gender and racial equality.

In contrast to this, however, a community group providing pandemic-related economic relief to a marginalized community consciously used an intersectional lens to analyze how their own response accounted for gender, age, disability, or class. This intersectional view was important for them in determining those who may face double marginalization and may need further assistance and resources throughout the pandemic. This lens is valuable for those engaged in data management processes, as they can refine their knowledge of how groups are impacted and better respond.

It is important to apply an intersectional lens of analysis when conducting an impact assessment of data management processes. For example, when undertaking the principle of "safety" as defined above in the digital literacy competency framework, an intersectional lens is vital for understanding social inclusion and assessing impacts on multiple identity factors.

However, there is progress on this within the Service, through the presence of a variety of initiatives such as the Call to Action on Anti-Racism, Equity, and Inclusion, and through workshops and events. An example of fostering this culture of reflection was in 2020 when CSIS hosted its first Expert Symposium on Addressing Unconscious Bias, Diversity, and Inclusion in National Security meant to be an annual event. At this event, panelists broke down the "plus" in GBA+ to discuss how intersectionality can be further understood. Therefore, it is important to continue this momentum and incorporate anti-bias understanding into digital literacy competencies.

SUMMARY OF RECOMMENDATIONS:

- Transparency in how internal leadership learns about data management bias to ensure that they are best placed to offer support to employee networks on equity and employees’ Individual Learning Plans.

- Engage marginalized community representatives to help cultivate a culture of reflection that is responsive to bias and incorporates an intersectional lens and lessons learned to address policy endemic issues.

- Ensure that engagement and learning from marginalized communities is a long-term goal or adopted on a long-term or permanent basis to emphasize commitment to organizational culture change and systemic approaches rather than one-off interventions.

- Digital literacy: Using internal Individual Learning Plans to advance knowledge on diversity, equity, and inclusion with data management. CSIS would also need to examine if this could expand to departmental support, as one interviewee from within CSIS referenced a need for “one-on-one department support” to ensure departments conform to standards and directives. This is an internal process change that CSIS may want to investigate further.

- Integration of digital literacy courses into Individual Learning Plans offered through Government of Canada Learning which would provide a standard foundational understanding Service-wide.

FRAGMENTATION ACROSS GOVERNMENT DEPARTMENTS

Avenues for Interoperability

The increasing amount of data collected on citizens is held in the jurisdictions of provinces, cities, and the federal government. Several interviewees reiterated that the Westminster system of government, which Canada is modeled after, provides for different governmental departments and agencies to be siloed and has allowed for flexibility in creating standards on how data is collected and shared. This is not conducive to cross-departmental collaboration and information-sharing on the issues of bias and ethical data management. This topic came up in nine of our interviews, with interviewees citing a need for increased interoperability. While the term interoperability was originally defined within the information technology sector to refer to the ability of computer systems to exchange and make use of information, the term has evolved to take into consideration broader social, political, and organizational factors. Taking this into account, we are using interoperability as the ability of *systems* to exchange and use information (Leal et al., 2019).

Multiple government respondents indicated that there is a need to increase avenues of communication across departments to increase information-sharing on questions around data management and conversations on how to remedy biases that have been ingrained within the system. Improving information sharing between agencies can help ensure standards on good data governance are more formalized and compatible across departments.

Although CSIS operates within the national security sector, which has special exemptions and is seemingly separate from other governmental operations and service delivery, our conversations with various government officials revealed that challenges stemming from the policy endemic issues we defined earlier are occurring across government. Particularly, on the *Directive on Automated Decision-Making,* TBS engaged with other agencies under the Ministry of Public Safety such as the Canada Border Services Agency (CBSA) and the Royal Canadian Mounted Police (RCMP), but CSIS was not involved in these consultations.

Therefore, it is useful for CSIS to think of themselves as part of a broader federal ecosystem that is working to overcome systemic issues that may cause harm to certain groups when either seeking service or protection from the government or may prevent them from doing so.

By shifting this mindset, CSIS reaffirms its mandate to ensure a safe Canada, and allows for engagement with other departments to leverage existing practices, while adapting them to the fit within the national security context.

Interview participants highlighted multiple initiatives across government that CSIS can leverage to increase its efforts to foster cross-departmental collaboration to overcome policy endemic issues. We see the potential for exploring increased interoperability with the following agencies:

Interoperability in New Zealand

In New Zealand, the Chief Data Steward, Chief Digital Officer and Chief Information Security Officer work under a partnership initiated by the Government Chief Digital Officer in 2015. The partnership also includes more than 20 agencies across government and 55 senior leaders. A partnership that houses the functions of data, security and digitalization enables a cross-sectoral conversation on the ways in which data can be leveraged but also what the emerging concerns and risks are.

STATISTICS CANADA

We identified Statistics Canada as a key avenue for interoperability. This emerged from an interview where one respondent saw Statistics Canada as an underutilized asset in the context of data management. As an organization, Statistics Canada has rigorous standards, practices, and mechanisms for ethical data management. Specifically, a representative from Statistics Canada highlighted the Necessity and Proportionality Framework as a critical practice to ensure a high-level of ethics in data management. This relates directly to section 12 of the *CSIS Act*, which states that data will only be collected to the extent that it is strictly necessary.

> "In terms of thinking through how to use data responsibly, Statistics Canada is an asset that should be used more."
>
> - Dr. Christopher Parsons

Another important finding from a Statistics Canada representative is the recognition that data must be informed by context. This principle can help individuals understand how to measure the quality of both the data, and its source. There is a clear opportunity for synergy between Statistics Canada and CSIS to strengthen these definitions and frameworks to ensure the Service's data management approaches are in line with ethical data management practices that reduce bias throughout the data lifecycle, which will lead to reduced harms towards historically marginalized groups.

TREASURY BOARD SECRETARIAT OF CANADA

From our findings, we identified two directives that demonstrate the potential to increase interoperability between CSIS and the Treasury Board Secretariat.

First, the *Directive on Automated Decision-Making* aims to address bias by monitoring and ensuring data quality, i.e., data that is accurate, recent, and peer-reviewed. One interviewer noted that in the context of CSIS, the directive does not necessarily align because the nature of the organization is grounded in data collection versus decision-making; however, as CSIS moves to adopt automated decision-making and advanced analytical tools to assist in its operations, there is room to incorporate some of the principles of this directive into CSIS' operations.

As mentioned earlier in the report, an AIA helps determine the impact level of an automated system, which takes into consideration system design, the algorithm, decision type, impact, and data. At each of these levels, it is critical for CSIS to consider how bias could intrude on each factor.

Formalizing this reflective check has the potential to ensure that precautions are taken to reduce any harm that may occur to individuals and communities, thereby mitigating the perpetuation of policy endemic issues. This also aligns with the Organization for Economic Cooperation and Development (OECD) Good Practice Principles for Data Ethics in the Public Sector, which reiterates the specificity around the purpose of data use and self-assessment and reflection tools to help define boundaries across the various aspects of the data lifecycle (OECD, 2021).

OECD GOOD PRACTICE PRINCIPLES FOR ETHICS IN THE PUBLIC SECTOR

The move towards digital government, increased data flows, and the difficulty of creating cross-border governance structures for data highlight the need for more granular policy guidance on the ethical implications of accessing, sharing, and using data (OECD, 2021). The emergence of new technologies has the potential for an exponential increase in data generation and use from digitalization of different aspects of society. This expands the possibilities for data analytics, with governments leveraging digital technologies to improve and streamline government functions, inform the design and delivery of improved policies and services, and automate decision-making processes through the use of algorithms (OECD, 2021).

The Good Practice Principles were produced by the OECD Working Party of Senior Digital Government Officials (OECD, 2021). These ten principles outline common actions for OECD members to follow, which place human rights and values at the core of digital government and data policies, strategies, projects and initiatives (OECD, 2021).

Through the development of values-based guidance governments are able to:

- Adopt inclusive and collaborative approaches to designing data policies, strategies, and initiatives – reinforcing the ethical use of data in the public sector
- Build consensus on how to foster public trust in practice in the context of data management
- Agree on trustworthy data management practices based on shared values

Second, the *Directive on Privacy Impact Assessment* provides direction to government institutions on how to evaluate the privacy impacts of programs or activities that deal with personal information. This directive makes it mandatory for a governmental agency to document, publish, and maintain a privacy impact assessment for any program or service that could impact privacy rights. The increasingly complex web of data and technology creates concerns for privacy, especially the use of surveillance technologies. In particular, the complexity of national security work and the necessity to collect information on potential threats allows for the intrusion of privacy of suspicious individuals or entities. If biases are not mitigated prior to data collection on certain suspicious individuals, then there is the potential for historically marginalized groups to experience disproportionate harm. Incorporating a privacy impact assessment before utilizing advanced analytical tools in national security, at both the individual and community level can pre-emptively mitigate any harm that may be experienced by historically marginalized communities. Formalizing privacy impact assessments with privacy protection at the forefront ensures that privacy protection is proactively considered and implemented before engaging in any data collection activities (Cavoukian, 2012 as cited in Strauss, 2019).

STANDARDS COUNCIL OF CANADA

Another way to increase interoperability is through standardization. Standardization is an effective way to facilitate conversations between systems. The fast-paced and innovative nature of data and technology pose challenges for legislation and regulations on privacy, but as one respondent stated, standardization helps build a bridge between the worlds of innovation and regulation. This emphasizes the role of standards in helping discover what absolutely must be regulated, and fosters conversations on what is a good practice. Something to consider when implementing standards is the potential for the reduction in nuance of lived experience.

> "Standardization helps with interoperability. Systems need to talk together."
>
> - Interviewee (Government Official)

Conformity to certain standards can help build trust, especially when they are grounded in values of trust, collaboration, and consensus. Building trust with communities through meaningful and inclusive engagement on standards development provides an avenue for which policy endemic issues can be overcome.

One respondent from the Standards Council of Canada elaborated on the work the organization is conducting with Indigenous communities through the *Data Governance Standardization Roadmap*. As data sovereignty is a sensitive subject for Indigenous communities, it is important to include these communities in conversation circles to create standards that are inclusive of the voices and perspectives of historically marginalized communities. In doing so, standards act as a mechanism that encourages trust between departments and other stakeholders. By developing standards for good data governance that are reflective of the values and diversity of all Canadian peoples through collaborative processes with various communities, standards provide a common language to enable cross-departmental conversations on issues of bias in data management practices.

SUMMARY OF RECOMMENDATIONS

- Champion a shift in organizational culture that centres reflexivity, collaboration, inclusivity, and ongoing learning. These principles are a critical launch point for the adoption of all other recommendations highlighted in this report.

- Create formalized cross-departmental (Statistics Canada, TBS, Office of the Privacy Commissioner, Standards Council of Canada) working groups to share how other agencies' bias mitigation approaches and principles for ethical data management have worked to date and can be modified to fit the national security context. Other stakeholders operating in the national security context like those under the Public Safety Canada portfolio like Correctional Services Canada, CSE, RCMP, and CBSA, and the Department of National Defence have guiding principles for data analytics and ethical frameworks that could be integrated into these cross-departmental working groups.

- Increase avenues for information-sharing on how standards for good data governance and bias mitigation are being incorporated.

CONCLUSION

This study affirmed that security and intelligence often have to perform a delicate balance between striving to be effective in their mandate to protect and remaining accountable to the governance structures that provide their mandates especially in a democratic context. Our research illustrated that this is even more complex given the intricacies of the data lifecycle and the endemic bias that is experienced and affect different stages of the data management process. However, in the same vein we also demonstrated that there is awareness of the need to mitigate the effects of bias in different stakeholder groups.

Recognizing this broad understanding is the first step for CSIS to reframe its efforts at mitigating the effects of data management bias as part of a larger ecosystem of stakeholders working on this issue. Seeing themselves as part of this larger ecosystem helps spotlight the efforts happening across government which overlap with the Service's mandate as enshrined in the *CSIS Act*. Within this action, there also exists an opportunity to re-think what protecting Canadians means as per the mandate. This would include expanding the duty to protect to include understanding the various vulnerabilities and resultant effects marginalized communities have experienced due to bias in data management practices historically.

With our scan of best practices from other contexts, literature review, and interviews, we came up with various recommendations that can be summarized as follows:

- Build on existing accountability mechanisms by engaging marginalized community voices both internally and externally.
- Bolster internal learning opportunities to incorporate digital literacy with awareness of endemic data bias issues to shift organizational culture.
- Increase interoperability by improving avenues for information-sharing on standards for good data governance and bias mitigation.

We believe this offers CSIS a set of solid starting points to continue the work of bias mitigation which centres an understanding of both endemic biases and the strategies already in use in various contexts.

GLOSSARY OF TERMS

AOSE Academic Outreach and Stakeholder Engagement

AI Artificial intelligence

AIA Algorithmic Impact Assessment

BIPOC Black, Indigenous, People of Colour

CBSA Canada Border Services Agency

CSE Communications Security Establishment

CSIS Canadian Security Intelligence Service

Data Bias the ways in which subjective assumptions regarding race, gender and other social groups are embedded within the collection and application of data

GBA+ Gender-based Analysis Plus

NSIRA National Security and Intelligence Review Agency

OECD Organization for Economic Cooperation and Development

RCMP Royal Canadian Mounted Police

TBS Treasury Board Secretariat of Canada

REFERENCES

"Beginning the Conversation A Made-in-Canada Approach to Digital Government". (2017). Beginning the Conversation – Full Report – Canadian Digital Service. https://digital.canada.ca/beginning-the-conversation/full-report/?fbclid=IwAR3p4ptcLDwQ6FJr4GW3PskHDsFuI2Gb1Ft23W-Jp-QOQrmZEAFZxHKx8dY.

Bejaković, P., & Mrnjavac, Ž. (2020). The importance of digital literacy on the labour market. *Employee Relations: The International Journal*, *42*(4), 921–932. https://doi.org/10.1108/er-07-2019-0274

Bowleg, L., & Bauer, G. (2016). Invited reflection. *Psychology of Women Quarterly*, *40*(3), 337–341. https://doi.org/10.1177/0361684316654282

Canada covid-19 app. Thrive Health. (n.d.). Retrieved February 3, 2022, from https://welcome.thrive.health/canada-covid19-app

Centering racial equity. Actionable Intelligence for Social Policy. (n.d.). Retrieved February 3, 2022, from https://www.aisp.upenn.edu/centering-equity/

Cho, S., Crenshaw, K. W., & McCall, L. (2013). Toward a field of intersectionality studies: Theory, applications, and praxis. *Signs: Journal of Women in Culture and Society*, *38*(4), 785–810. https://doi.org/10.1086/669608

Christoffersen, A., & Hankivsky, O. (2021). Responding to inequities in public policy: Is GBA+ the right way to operationalize intersectionality? *Canadian Public Administration*, *64*(3), 524–531. https://doi.org/10.1111/capa.12429

Consolidated federal laws of Canada, Canadian Security Intelligence Service act. Canadian Security Intelligence Service Act. (2022). Retrieved February 3, 2022, from https://laws-lois.justice.gc.ca/eng/acts/c-23/page-2.html#h-76283

Costanza-Chock, S. (2020). *Design justice: Community-led practices to build the worlds we need*. The MIT Press.

Crenshaw, K. (1991). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review*, *43*(6), 1241. https://doi.org/10.2307/1229039

Data Lifecycle. Data Lifecycle | U.S. Geological Survey. (n.d.). Retrieved February 3, 2022, from https://www.usgs.gov/data-management/data-lifecycle

Digital Competence Framework 2.0. EU Science Hub. (n.d.). Retrieved March 4, 2022, from https://joint-research-centre.ec.europa.eu/digcomp/digital-competence-framework-20_en.

Government of Canada/Gouvernement du Canada. (2021). WGEC Government of Canada. Women and Gender Equality Canada. Retrieved March 4, 2022, from https://women-gender-equality.canada.ca/en/gender-based-analysis-plus.html.

Government of Canada/Gouvernement du Canada. (2020). Canadian Security Intelligence Service, Government of Canada. Canada.ca. Retrieved February 3, 2022, from https://www.canada.ca/en/security-intelligence-service/corporate/legislation.html

Government of Canada/Gouvernement du Canada. (2021). Passenger Protect Program (PPP). Canada.ca. Retrieved February 28, 2022, from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/pssngr-prtct/pssngr-prtct-prgrm-en.aspx.

Government of Canada/Gouvernement du Canada (2021). Government of Canada. Canada.ca. Retrieved Feb 3, 2022, from https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html

Johnson, Phil, and Joanne Duberley (2003) “Reflexivity in Management Research.” Journal of Management Studies 40(5) 1279 – 1303.

Krafft, P. M., Young, M., Katell, M., Lee, J.E., Narayan, S., Epstein, M., Dailey, D., et al. (2021). An Action-Oriented AI Policy Toolkit for Technology Audits by Community Advocates and Activists. In Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 772–81. Virtual Event Canada: ACM. https://doi.org/10.1145/3442188.3445938.

Leal, G., Guédria, W., Panetto, H. (2019). Interoperability assessment: A systematic literature review. Computers in Industry, 106, 111-132. https://doi.org/10.1016/j.compind.2019.01.002.

Lopez, P. (2021). Bias does not equal bias: A socio-technical typology of bias in data-based Algorithmic Systems. Internet Policy Review, 10(4) https://doi.org/10.14763/2021.4.1598

McGregor, L., Murray, D., & Ng, V. (2019). International human rights law as a framework for algorithmic accountability. International and Comparative Law Quarterly, 68(2), 309–343. https://doi.org/10.1017/s0020589319000046

Mythen, G., Walklate S., & Fatima, K. (2009). ‘I’m a Muslim, But I’m Not a Terrorist’: Victimization, Risky Identities and the Performance of Safety.” The British Journal of Criminology 49 (6): 736-754. https://www.jstor.org/stable/23639597

No Fly List Kids. (2017). Written Submission on Bill C-59 to Standing Committee on Public Safety & National Security. https://www.ourcommons.ca/Content/Committee/421/SECU/Brief/BR9624963/br-external/NoFlyListKids-e.pdf.

National Security and Intelligence Review Agency. (n.d.). What We Do. Retrieved April 2, 2022, from https://nsira-ossnr.gc.ca/what-we-do.

National Security and Intelligence Review Agency. (2019). Review of the Canadian Security Intelligence Service's (CSIS) use of Geolocation information. Retrieved April 17, 2022, from https://nsira-ossnr.gc.ca/nsiras-review-of-the-canadian-security-intelligence-services-csis-use-of-geolocation-information.

OECD. (2021). Good Practice Principles for Data Ethics in the Public Sector. https://www.oecd.org/digital/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm.

Office of the Privacy Commissioner. (2020). 2020-21 Survey of Canadians on Privacy-Related Issues. Retrieved April 17, 2022, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/#toc2-1.

Office of the Privacy Commissioner. (2015). A Guide for Individuals - Protecting Your Privacy. Retrieved April 2, 2022, https://www.priv.gc.ca/en/about-the-opc/publications/guide_ind/.

Office of the Privacy Commissioner. (2021). Guidelines for obtaining meaningful consent. Retrieved April 17, 2022, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/#fn16-rf.

Paullada, A., Inioluwa D. R., Bender E. M., Denton, E., & Hanna, A. (2021). Data and Its (Dis)Contents: A Survey of Dataset Development and Use in Machine Learning Research. Patterns 2 (11): 100336. https://doi.org/10.1016/j.patter.2021.100336.

Parsons, C. (2020) Electronic Surveillance: The Growth of Digitally Enabled Surveillance and the Atrophy of Accountability in Law Enforcement and Security Agencies. In Digital Policies in Canada: Promises and Realities, edited by Small, T. A., & Jansen, H.J. Toronto: University of Toronto Press.

Priisalu, J., & Ottis, R. 2017. “Personal Control of Privacy and Data: Estonian Experience.” Health and Technology 7 (4): 441–51. https://doi.org/10.1007/s12553-017- 0195-1.

Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018). Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability. AINOW Institute. https://ainowinstitute.org/aiareport2018.pdf

Republic of Estonia Information System Authority. (2022). Estonian Information Security Standard. Retrieved February March 5, 2022, from https://www.ria.ee/en/cyber-security/estonian-information-security-standard.html

Robertson, K., Khoo, C., & Song, Y. (2020). To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada. Toronto: The Citizen Lab https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/

Secretariat, T. B. of C. (2021). Government of Canada. Canada.ca. Retrieved Feb 3, 2022, from https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html

Strauss, S. (2019). How to regain control? In Privacy and Identity in a Networked Society (188-230). Routledge.

Theilen, J. T., Baur, A., Bieker, F., Quinn, R. A., Hansen, M., & Fuster, G. G. (2021, December 7). Feminist Data Protection: An introduction. Internet Policy Review. Retrieved Feb 3, 2022, from https://policyreview.info/articles/analysis/feminist-data-protection-introduction

Tsalikis, C. (2020). At Canada's spy agency, a new women's Network Safeguards Progress on Gender Equality. Open Canada. Retrieved March 4, 2022, from https://opencanada.org/at-canadas-spy-agency-a-new-womens-network-safeguards-progress-on-gender-equality/