Face Recognition Technology for the Protection of Canada's Parliamentary Precinct and Parliament Hill?

POTENTIAL RISKS AND CONSIDERATIONS

Yuan Stevens, Ana Qarri, Sam Andrey, and Joe Masoodi | April 2022

LEADERSHIP LAB>>>

How to Cite this Report

Yuan Stevens, Ana Qarri, Sam Andrey and Joe Masoodi. (2022). Face Recognition Technology for the Protection of Canada's Parliamentary Precinct and Parliament Hill? Potential Risks and Considerations. https://www.ryersonleadlab.com/frt-parliament-hill.

350 Victoria St, Toronto, ON M5B 2K3

LEADERSHIP LAB>>>

The Leadership Lab is an action-oriented think tank at Toronto Metropolitan University (formerly Ryerson University) dedicated to developing new leaders and solutions to today's most pressing civic challenges. Through public policy activation and leadership development, the Leadership Lab's mission is to build a new generation of skilled and adaptive leaders committed to a more trustworthy, inclusive society.
For more information, visit ryersonleadlab.com or @TMULeadLab.

Table of Contents

Acknowledgments

The authors of this study wish to thank the Parliamentary Protective Service for the invitation to undertake this important research. They also extend gratitude to all of the PPS staff members who, through interviews, shared their knowledge of how the PPS does its vital work. We thank all those we spoke to for their openness and for respecting the independent nature of this study.

The authors of this study are also grateful to Alessandra Puopolo for assistance with background legal research, to Cathy McKim for copy editing, to André Côté for help and support with project management, and to Zaynab Choudhry for support with design. They also wish to thank Professor Philippe Lagassé for providing critical background knowledge on parliamentary privilege and the Westminster system of governance, areas of law and political science that the authors previously did not think could be as fascinating as they are. The authors would also be remiss not to thank Professors Pete Fussey and Daragh Murray for shedding light on considerations and good practices for examining the human rights impacts of face recognition technology in the public safety context. Unless otherwise specified, the findings and opinions of this report are those of the authors alone, as are any of the report's shortcomings.

The authors would also like to express gratitude to the experts who provided insight and expertise that informed this report through in-depth interviews:

- **Suzie Dunn** (Schulich School of Law, Dalhousie University)
- **Albert Fox Cahn** (Surveillance Technology Oversight Project)
- **Pete Fussey** (Department of Sociology, University of Essex)
- **Martin Innes** (Crime and Security Research Institute, Cardiff University)
- **Tamir Israel** (Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, Faculty of Law, University of Ottawa)
- **Rosel Kim** (Women's Legal Education and Action Fund)
- **Shoshana Magnet** (Feminist and Gender Studies, Faculty of Social Sciences, University of Ottawa)
- **Matt Mahmoudi** (Amnesty International and University of Cambridge)
- **Daragh Murray** (Human Rights Centre & School of Law, University of Essex)
- **Benjamin Muller** (Department of Political Science, King's University College, University of Western Ontario)
- **Brenda McPhail** (Privacy, Surveillance, and Technology Project, Canadian Civil Liberties Association)
- **Tim McSorley** (International Civil Liberties Monitoring Group)
- **Christopher O'Connor** (Criminology and Justice, Faculty of Social Science and Humanities, Ontario Tech University)
- **Kanika Samuels-Wortley** (Department of Criminology, Toronto Metropolitan University)
- **Andrea Slane** (Legal Studies, Faculty of Social Science and Humanities, Ontario Tech University)
- **Cee Strauss** (Women's Legal Education and Action Fund)
- **Leah West** (Norman Paterson School of International Affairs, Carleton University)

Executive Summary

This report was prepared at the request of the Parliamentary Protective Service to examine the human rights and legal considerations for the hypothetical use of face recognition technology (FRT) in the context of ensuring physical security within Canada's parliamentary precinct and on Parliament Hill. It demonstrates that there are substantial legal, privacy, and human rights risks associated with the use of FRT. Faces are a type of biometric information unique to each person, and FRT determines the probability of facial similarity in images through computational analyses. Faces reveal who we are, where we come from, our families of origin, and can reveal other aspects of our lives such as our gender, race, ethnicity, health, and emotions — along with highly personal or intimate information about our lives such as our relationships, political or personal preferences, and travel patterns, particularly when our faces are examined over time. While this report focuses on the use of face recognition in the parliamentary context, it has numerous lessons that may apply to other physical security approaches including the use of biometric recognition systems.

There are currently no clear legal limits nor required safeguards regarding the collection and processing of biometric information such as facial images through automated means — a major gap in Canada's privacy and human rights legal framework. Despite this, it is possible that the potential use of FRT in the parliamentary context, particularly for the unique identification of people through one-to-many searches, could be found unlawful and may affect the public's trust and confidence that their privacy and other rights are being adequately protected and prioritized by their democratic institutions. This is because FRT can surveil, track, identify, misidentify, and may lead to decisions that result in people being stopped, questioned, detained and/or prevented from entry to the parliamentary precinct and Parliament Hill at significant scale and speed and in ways that are discreet and potentially arbitrary.

Algorithmic systems such as FRT reproduce and exacerbate the values and biases held by the people who create and use such systems. As a result, there is no such thing as algorithmic systems with "neutral" or "objective" results, because human biases are built into all aspects of the design of technology, such as the historical data on which a system is trained, how that data is gathered and labelled, and the construction of watchlists. The accuracy issues of FRT systems also relate to and can exacerbate the discriminatory impacts of such technology.

Parliamentary privilege — that is, the powers and immunities available to parliamentarians needed to do their work — should play a prominent role in any decisions regarding the use of FRT in the parliamentary context as well as the conditions of any deployment. This privilege can be pointed to by PPS with a view to justify the use of certain physical security and surveillance measures such as FRT, with the potential result that the *Charter of Rights and Freedoms* or other laws could not be invoked regarding the use of this measure. However, FRT could potentially be used with the effect that it impedes or delays parliamentarians from accessing Parliament or impedes certain parliamentarians more than others due to the potential discriminatory impacts of FRT, which may challenge the ability for PPS to rely on the privilege that exists to enable parliamentarians to perform their work.

FRT poses significant concerns to the public from a privacy perspective. The use of FRT can disrupt the ability for visitors to remain anonymous and move freely at Parliament. The technology can be used to uniquely identify individuals who visit Parliament or categorize them based on their identity and, after identifying people, can be used to track their location patterns, political leanings, personal preferences, and activities. It can erode privacy rights enshrined in the *Charter* under section 8 and in the *Privacy Act*. When privacy rights are eroded, this paves the way for other rights under the *Charter* to be violated.

The potential use of FRT in the parliamentary context also raises numerous risks regarding the right to free expression, freedom of assembly, and association. Some of Canada's most vulnerable populations visit Parliament to participate in rallies, protests, and to make their voices heard on essential political issues, which are activities that the PPS plays a key role in facilitating and protecting. The use of FRT can give rise to chilling effects that are likely to dissuade many groups from organizing and visiting Parliament on critical issues — particularly for communities such as Black and Indigenous people who have been historically subject to increased state surveillance. It is worth considering whether the impacts of FRT on these fundamental freedoms would be antithetical to the Canadian and democratic values that Parliament represents.

FRT also poses concerns in light of equality rights under section 15 of the *Charter* and other laws that may apply. FRT has higher inaccuracy rates for racialized individuals and others belonging to historically marginalized groups. If a security entity were to act on such outputs, the action could very well be a violation of the individual's section 15 equality rights. Even if FRT were to be perfectly accurate, discrimination may be embedded in the databases upon which an FRT system is trained and used and how personnel act upon the system's findings. This is due to concerns that FRT system watchlists remain comprised of people who are disproportionately represented in other watchlist databases used by public safety and intelligence agencies, which is a product of the historic over-policing of these communities.

It is therefore clear that the legal, privacy, and human rights risks associated with FRT are numerous. If there is a decision to use FRT in the parliamentary context despite these risks, the following non-exhaustive set of considerations may serve useful:

- **The Principles of Necessity, Proportionality, Effectiveness, and Minimal Impairment:** The principles of necessity, proportionality, and their related considerations of effectiveness and minimal impairment ought to inform the collection and processing of facial information through FRT in the parliamentary context. Applying these principles for any potential deployment of FRT is critical for specifying, in an evidenced-based manner, whether FRT is needed in the parliamentary context, as well as its risks related to privacy and relevant *Charter* rights.
- **Impact Assessments:** Transparent impact assessments focused on privacy, the risk of *Charter* infringements, and automated decision-making or recommendation systems would be important to undertake both prior to the use of FRT and, if it is nonetheless used, on an ongoing basis post-implementation. This should include ensuring, for example, that information used from third parties was collected lawfully, and that minimum accuracy and bias thresholds are in place.

- **Purpose Limitation:** Clear and firm policies that narrowly scope how, when, where, and why FRT is used would be a first general set of steps that should be used in mitigating the technology's risks. These limits include crafting specific, targeted purposes or triggers for its use; temporal limits on its use; limiting its use to the fewest geographic locations or to specific locations; and limiting whose facial images are scanned, compared, and stored.
- **Public Consultation and Notice:** Given that FRT has the ability to facilitate the infringement of people's *Charter* rights, the public should be consulted and explicitly notified regarding the use of FRT in the parliamentary context should it be used despite the risks it poses. Prior to use, particular consultation should be conducted with communities that stand to be the most affected by the use of this technology, including people of colour, religious minorities, people from the LGBTQ2+ communities, people with disabilities, and others.
- **Information Collection and Retention:** To justify the collection of highly sensitive biometric information such as faces and the templates that can be made of a person's face, there needs to be a demonstrable need to collect and retain each piece of information. If FRT is used, any facial templates collected beyond a demonstrable need should be deleted immediately; and, if stored, should be de-identified to be in line with best practices regarding the storage of biometric information and to reduce the risk of privacy intrusions.
- **Sufficient Resources:** Significant resources are required for implementing face recognition systems, including for software, hardware, public consultation, technical and human rights auditing of the technology, and employee training on lawful use.
- **Human Intervention in Decision-Making:** It is important to have a trained human assess and validate any matches provided by an FRT system before action is taken based on that match, such as detaining someone or limiting their entry into a geographic area, as such actions may implicate the rights to due process or procedural fairness, as well as the right to freedom from arbitrary detention.

Certain uses of FRT could potentially address some, though not all, of the risks associated with the technology. For example, it could be possible that live FRT could pose fewer privacy-related concerns if used for authentication purposes through one-to-one searches at indoor entrances into buildings with good lighting — and only when the facial images of a smaller, select, and fixed group of people are collected, processed, and immediately discarded, such as parliamentary staff members or parliamentarians who knowingly opt into its use. However, the other concerns raised throughout this report, such as parliamentary privilege, as well as accuracy and bias concerns for minority populations, may nonetheless remain in this context.

Additionally, when FRT is deployed in a particular setting such as for the protection of parliamentarians and Parliament Hill, then the possibility and implications of scope or function creep are a significant concern. Once systems are in use for a narrow and specific purpose, it would not be difficult to expand their use for broader purposes or in a wider range of circumstances that nonetheless raise the risks outlined in this report, with the potential concomitant harms associated with these legal and human rights risks. The use of FRT by one institution can also legitimize its use in other contexts and by other entities, including where there are fewer safeguards in place to prevent its deleterious impacts, misuse, and abuse.

1.

About this Report

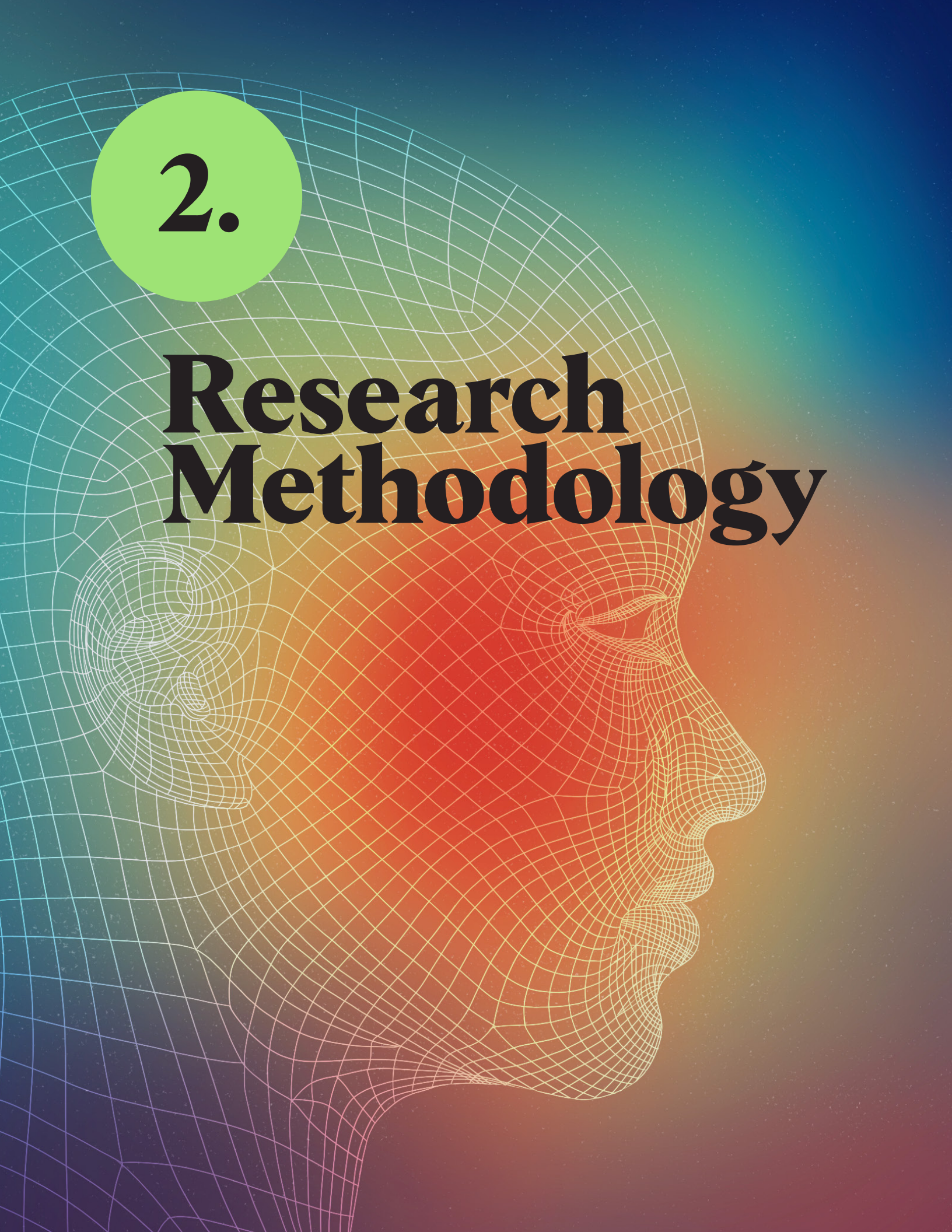
About This Report

Government institutions across the globe are increasingly expressing interest in automated biometric recognition systems in hopes of improving the efficiency of their services. A prominent example of such biometric recognition software includes face recognition technology (FRT). FRT uses computational analyses to determine the probability of facial similarity in images, and can do so discreetly at significant speed and scale. This report examines key human rights and legal considerations of the potential use of FRT in the context of Canada's parliamentary precinct and Parliament Hill. While this report focuses on the use of face recognition in the parliamentary context, it has numerous lessons that apply to biometric recognition systems more broadly.

Our research team from the Leadership Lab at Toronto Metropolitan University prepared this report for the Parliamentary Protective Service (PPS) between October 2021 and April 2022. The team agreed to produce an independent report based on interdisciplinary legal research and data gathered through interviews with PPS staff members, as well as lawyers, scholars, and practitioners with expertise on FRT or a related subject matter. The PPS funded this independent report; however, there were no data-sharing requirements between the research team and the PPS.

In interviews with PPS staff members, confidential information was obtained on the security practices used by the PPS. This report therefore speaks in purely hypothetical terms regarding the use of FRT in the parliamentary context. A draft version of this report was also submitted to the PPS in April 2022, so that any confidential information could be noted and redacted from this report prior to sharing it with the public. No such information has been redacted. Additionally, the PPS provided clarifications regarding certain sections of the report, which are provided in **Appendix A.**

Sharing this report with the public is important given the role of Canada's Parliament in facilitating democracy and the public's interest in understanding the impacts of technology used for physical security in this setting. Unless otherwise specified, the findings and opinions of this report are those of the authors alone, as are any of the report's shortcomings.



2. Research Methodology

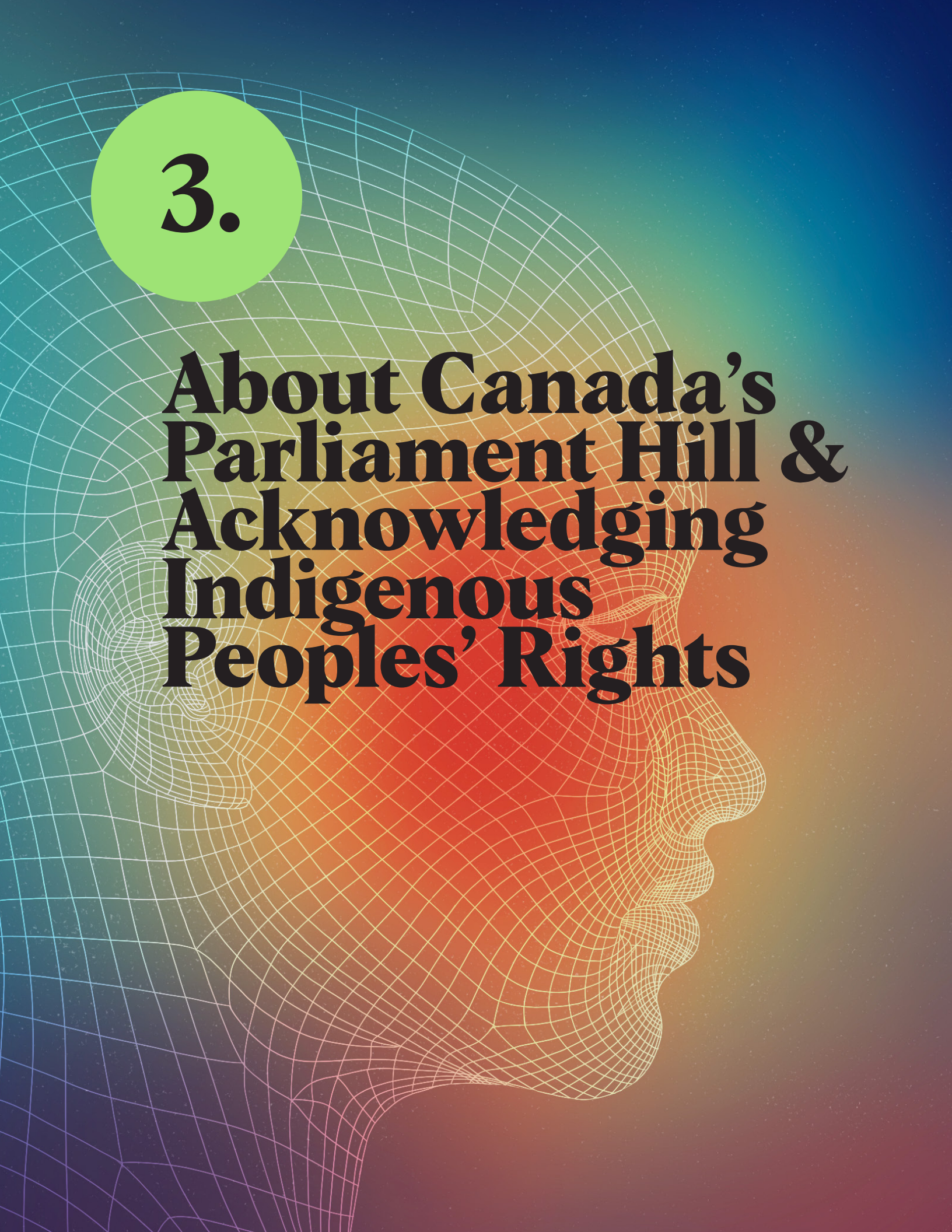
Research Methodology

This report examines the impacts or risks associated with the potential use of FRT by the Parliamentary Protective Service to physically secure Canada's parliamentary precinct and Parliament Hill. This study considers and explores the following question: what considerations ought to guide the potential procurement and use of FRT in the parliamentary context from a legal, ethical, privacy, and security perspective?

Interdisciplinary methods were used to answer this question. The research team analyzed relevant secondary literature regarding the use of FRT for public safety, drawing on the fields of law, computer science, surveillance studies, and sociology published in or around 2010 and later. Legal analysis was also undertaken, with a focus on the privacy and human rights implications of FRT. Areas of law examined include the role of parliamentary privilege, international human rights law where relevant, constitutional law (including the *Canadian Charter of Rights and Freedoms*), and privacy law. A review of policy best practices related to privacy, human rights, cybersecurity, and other relevant considerations was also completed, and the resulting key considerations are found in the report's executive summary and at the end of each section. This interdisciplinary legal and human rights analysis was important for addressing the impacts and risks of FRT in the parliamentary context.

The researchers also conducted qualitative, semi-structured interviews in the months of January-March 2022 as reviewed by Toronto Metropolitan University's Research Ethics Board. A total of 32 people were interviewed. Interviews were conducted with 15 members of PPS staff who have knowledge of current security practices and/or organizational norms. An additional 17 experts were interviewed external to the PPS, hailing from various sectors — including academia, law, and civil society — with expertise on topics such as the efficacy and impacts of face recognition, privacy law, human rights law, criminology, surveillance studies, and organizational best practices regarding the use of technology. A mixed sampling strategy was used to select interview participants external to the PPS, including purposive, convenience, and snowball sampling.[1] The research team sought to interview a diverse set of external experts in terms of gender, race and ethnicity, and sector or field of study. Such in-depth interviews were chosen to inform analysis of the implications and risks of FRT, as well as considerations regarding potential deployment. A visit to the parliamentary precinct and Parliament Hill was also planned to facilitate observation as part of the methods used for this study, but was unfortunately unable to happen due to the 2022 convoy protest that occurred in Ottawa and the COVID-19 pandemic.

Interviews lasted between 45 and 60 minutes, and were held virtually through Zoom or Microsoft Teams. Interview questions generally focused on existing practices with respect to securing government buildings, interviewees' knowledge of FRT, how the technology is currently being used by different actors, the laws and organizational policies and best practices that shape its use, and organizational considerations regarding use of this technology by the PPS and in a Canadian context more broadly. A reflexive approach informed the interview process wherein researchers acknowledged their role as participants in the process of knowledge construction.[2] Interviews were audio-recorded and transcribed when consent was provided by the interview subject. Only the authors of this report have access to the complete audio and transcription files. Data gathered from all interviews provided only background knowledge useful for the drafting of the report. The names of PPS staff interviewed for this report are not included in the acknowledgments section of this report to respect the consent of those interviewed, while the list of experts external to the PPS is included with the permission of all those listed.



3.

About Canada's Parliament Hill & Acknowledging Indigenous Peoples' Rights

About Canada's Parliament Hill and Acknowledging Indigenous Peoples' Rights

Parliament Hill is one of the most important places within Canada. It is the physical embodiment of Canada's federal government system and of our democracy. Indeed, it is "the very heart of Canada's democratic system of government."[3] It houses the executive, legislative, and judicial branches of the state. The collection of buildings on Parliament Hill are "shrines to our freedom."[4] The Supreme Court of Canada has concluded that Parliament Hill "is a powerful symbol of Canada, representing our democratic tradition both to its citizens and residents, as well as to the millions of visitors who come to this country each year."[5]

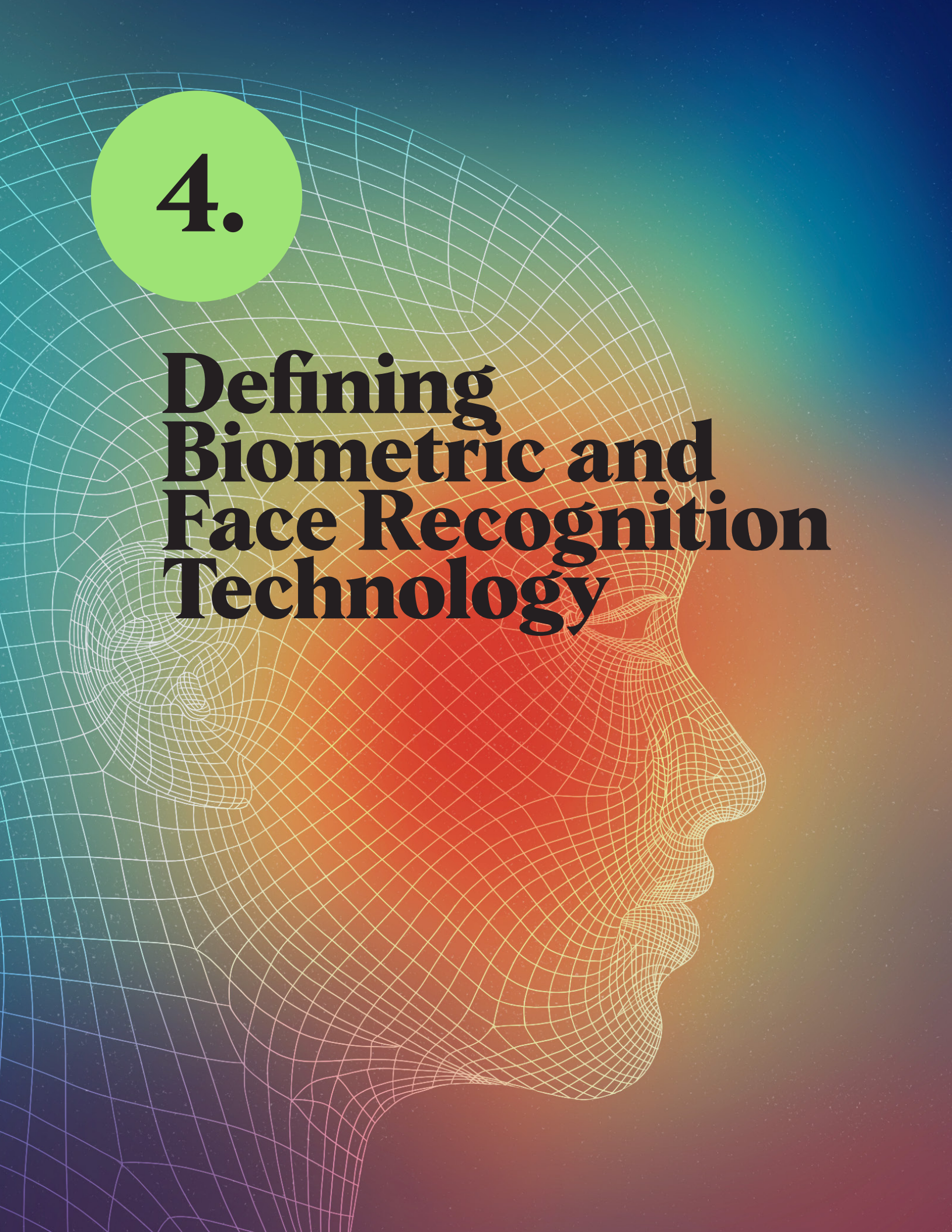
Many visitors to Parliament Hill and the parliamentary precinct visit as tourists, but many others visit for meetings with Members of Parliament and other government officials.[6] Still others visit Parliament Hill and its precinct to engage in political expression, ranging from activities such as vigils regarding violence against women,[7] demonstrations relating to healthcare,[8] or demonstrations regarding rights for people with disabilities.[9] Visitors to Canada's parliamentary precinct and Parliament Hill can include some of the country's most vulnerable communities.

It must also be acknowledged that Indigenous communities inhabited this land long before the arrival of European settlers. In particular, the southern banks of the Ottawa River (on which Canada's parliamentary precinct resides) have been an important site for various Indigenous and First Nations communities, particularly the Algonquin Nation.[10]

Discussing the security of Canada's Parliament would therefore be incomplete without acknowledging the significant and longstanding harm that has been perpetrated against Indigenous peoples through state action.[11] For over 150 years, Canadian policies and legislation have sought to control Indigenous communities and have destroyed their cultures, ways of life, and forms of governance.[12] This process of assimilation has aimed to ignore Indigenous peoples' rights, as well as rob them of their distinct identities through actions such as the assertion of control over land and the hyper-surveillance of Indigenous peoples.[13]

Canada is still in the process of reckoning with its colonial history. More recently, shockwaves were felt around the nation — and on a global scale — when more than one thousand mass unmarked graves were discovered at former residential schools across Canada in 2021.[14] Spurred on by this discovery, the Prime Minister explicitly referenced in all of his 2021 mandate letters the need for each minister to implement the *United Nations Declaration on the Rights of Indigenous Peoples* and to work in partnership with Indigenous communities to advance their rights.[15] The Truth and Reconciliation Commission Calls to Action also call upon the federal government to commit to eliminating the over-representation of Indigenous peoples and young people in custody — an important consideration when examining surveillance and security approaches and their intersection with public safety.[16]

In light of this, we acknowledge the urgent need to centre the rights and interests of Indigenous peoples in our analysis of the human rights implications related to the potential use of face recognition technology at Canada's Parliament Hill and parliamentary precinct. We similarly urge all readers of this report, including members of PPS, to do the same as they read our report's findings and implement or learn from its conclusions.



4.

Defining Biometric and Face Recognition Technology

Defining Biometric and Face Recognition Technology

Faces are one of the most important physical parts of who we are as individuals. They are unique to us. Our faces generally remain unchanged throughout our lives.[17] Faces reveal who we are, where we come from, our families of origin, and can reveal other aspects of our lives such as our gender, race, ethnicity, health, and emotions — along with highly personal or intimate information about our lives such as our relationships, political or personal preferences, and travel patterns, particularly when our faces are examined over time.

Faces are a type of biometric information or data.[18] Biometric information is data related to the body or human characteristics. Scientists and industry actors have developed techniques, tactics, and technology that can compare patterns in biometric datasets.[19] These biometric analysis techniques produce outputs that identify when a certain threshold of similarity exists between biometric data. While we caution against anthropomorphizing such mathematical processes,[20] such techniques and technology can be seen as 'recognizing' patterns between biometric data that is stored and new biometric data that has been collected. This report uses the shorthand 'biometric recognition technology' to capture software with such capabilities. Technology that 'recognizes' patterns in faces is a subset of biometric recognition technology and is referred to in the scientific community as facial or face recognition technology.

Experts distinguish between the analysis of 'strong', 'weak', and 'soft' biometric data.[21] 'Strong biometrics' refers to the analysis of data that is generally unchangeable and unique to a given person. Examples include genetic material, fingerprints, palm prints, voices, and irises. Faces are a type of 'strong' biometric data. 'Weak biometrics' refers to the analysis of data that is less fixed in nature and generally reveals less fixed states that may still be attributed to a particular person. Examples include a person's body shape, behavioural patterns such as gait, and body sounds. 'Soft biometrics' refers to features that are generic in nature and that are not uniquely associated with an individual, including gender and age, for example.

Biometric recognition technology functions through the comparison of stored and live biometric prints or 'templates.'[22] A fingerprint is an example of such a template. Templates require the measurement of various aspects and features of biometric data. For facial images, systems typically measure and compare elements such as the colour and hue of the pixels within an image, the distance between facial features (such as eyes, mouth, chin, eyebrows, etc.) and the alignment between aspects of images.[23] Stored templates comprise the dataset or datasets against which live templates are compared.

Stored templates function as 'watchlists' when public safety actors use them to identify people who have been flagged as safety or security risks. Landmark work in 2019 by Pete Fussey and Daragh Murray on the London Metropolitan Police's use of FRT demonstrates that a critical issue is the criteria used for the construction of watchlists and the criteria used to compile them.[24] Understanding how watchlists are constructed is vital for determining the legality of such lists and for ascertaining the human rights impacts of a given face recognition system. For example, the legality surrounding the construction of an FRT system's watchlist was a key issue

in a recent decision by the Office of the Privacy Commissioner (OPC). In 2021, the OPC concluded that facial image databases and watchlists are to be collected only through lawful means, as explained further in **Section 6.1.1.**[25] The quality of images found in a watchlist is also another consideration related to an FRT system's accuracy, as further explained in **Section 4.1.**

Biometric recognition technology can be used to authenticate a person's known identity or to uniquely identify a person's identity when they are not yet known.[26] Authentication occurs when someone claims to be a particular person and provides a live biometric template to compare against their own stored template in order to confirm their identity. In other words, authentication involves a person's specific biometric template being compared against their own stored template. As such, this constitutes a '**one-to-one**' comparison. A good example of biometric recognition technology being used for authentication includes the storage of a person's thumbprint or facial template on a device, which is compared to the live template of their own biometric template in order to obtain access to the device.

In contrast, biometric and face recognition technology can be used to categorize or uniquely identify an unknown person.[27] When FRT is used for such categorization or identification purposes, a person's live facial template is compared against a database of many other facial templates, also known as a '**one-to-many**' comparison. In this context, FRT can be used to categorize a person based on perceived features such as their gender, ethnicity, age, and the like. FRT can also be deployed with a view to uniquely identify a person based on the similarity of their facial template to stored templates found in a watchlist or set of watchlists. Some databases may contain millions or even billions of templates. When there are this many templates, it is possible that there will be duplicate images or templates of the same person.

Biometric recognition technology can be used to compare and produce results in real-time in a live setting or for investigation after alleged wrongdoing has occurred with static images, also referred to as 'live' and 'retroactive' FRT, respectively. For example, when FRT is used for the unique identification of people in real-time, cameras deployed will constantly be scanning live video feeds for faces, and comparing facial images captured with databases of stored facial templates.[28] Recommended matches will be produced within a matter of seconds or minutes.

When UK police forces in London and Cardiff used FRT in live settings, FRT operators could decide the minimum level of accuracy required for recommended matches to pull up.[29] The operators involved needed to confirm whether they believed the match or matches were correct, and would proceed to attempt to apprehend the person or engage with the individual on the basis of the information associated with the face-match alert. It is worth noting here that the UK Court of Appeal concluded in 2020 that the use of FRT in real-time by the South Wales Police was illegal because it violated privacy rights, data protection laws, and the right to equality or freedom from discrimination.[30]

Biometric and face recognition can also occur retroactively on static images. When it comes to FRT, this could look like comparing a recently submitted driver's licence photo with a database of driver's licence photos when the comparison does not happen in real-time. It could also involve the extraction of facial images from video recorded via CCTV and comparison of the facial images with a watchlist. In the public safety context, the primary difference between the use of

FRT in real-time or after alleged wrongdoing has occurred involves the speed with which a person can be excluded from a geographic location, or their liberty deprived by being detained or arrested.

4.1 The Development and Functioning of FRT Systems

To understand the implications of FRT, it is important to understand how such systems are developed and the high-level fundamental details of how they function. Biometric and face recognition systems are computer programs made up of algorithms, inputs (e.g., training data, stored templates, live templates), and outputs (recommended matches).

Algorithms, understood at their simplest, are sets of rules of instructions. Analogue examples include recipes or patterns for making a piece of clothing. Digital examples include lines of computer code that include logical if-then statements, which tell a computer system to execute tasks in a particular order using certain variables and inputs. Different systems' algorithms perform differently and are associated with varying accuracy rates.[31] For example, the South Wales Police used one company's FRT systems that used different algorithms at different times.[32] The different algorithms had different accuracy rates, with the later algorithms performing somewhat better than the first set used.

Computer code and the algorithms they contain can be open-source and available for all people to examine for transparency, and to assess design and security vulnerabilities. Computer code can also be proprietary and withheld from the public as a means to help ensure security and for economic viability. When two police forces in the UK trialled real-time FRT, they used software that was proprietary in nature, and it was therefore not possible to know how the software produced its matches. Proprietary software is appealing for organizations and companies that want to limit who can use and recreate their software; however, it can at times be far more challenging, if not impossible, for anyone who did not produce the software to understand the functioning of such proprietary technology and to assess the risks it may pose.

In terms of cybersecurity, closed-source software must be internally vetted for security flaws.[33] Proprietary systems also implicitly rely on 'security through obscurity', an approach that uses the secrecy of a system's functioning as a mode of defence from attack. A major weakness of proprietary, closed-source computer code concerns the lack of transparency regarding its functioning, particularly when things go wrong. The security of such systems can also be harder to guarantee. On the other hand, open-source computer code is appealing for its transparency, as such code can be reused, reworked, and easily examined in the open for its functioning and flaws. The downsides of open-source software are also its strengths, in that it is possible for anyone to know and take advantage of weaknesses that are out in the open; and the economic and informational control of open-source code is enabled through flexible open-source software licences.

Biometric and face recognition systems were born out of the field of artificial intelligence (AI). AI refers to multiple fields of study that explore how computers can be trained to execute instructions and tasks in ways that are similar to human intelligence.[34] The field emerged in the post-WWII environment; and significant advancements have occurred over the last few decades due to the creation and dissemination of massive amounts of data,

as well as increases in computer processing power.[35] AI can be 'narrow' or 'general', with the former referring to the development of systems for a specific purpose and the latter referring to systems that can perform multiple functions at once. Face recognition falls within the category of narrow AI and is a subset of image recognition (or what computer scientists refer to as 'computer vision').

Machine learning and other data science techniques can involve 'supervised' or 'unsupervised' learning, or a hybrid of the two.[36] Image recognition systems built through supervised learning must be developed using training datasets. In supervised learning, this data is labelled.[37] Elements of an image will be labelled, such as measurements between objects, colours, outlines, or pixels. In the context of face recognition, FRT systems will be trained to categorize or recognize patterns in new inputs, such as stored facial templates and new, live templates. There are many facial image datasets available that can be used to train an FRT system[38] and used for watchlists. However, significant legal issues exist around the legality of such databases. In many cases, images have been scraped from the web or repurposed from webcam and CCTV livestreams, for example, without the consent of the people depicted.[39]

Unsupervised learning systems are developed with datasets that are not labelled. With unsupervised learning, no particular outputs are sought and the system must identify patterns in datasets without initial human intervention — and, as a result, there can be difficulties in determining the bases for any biased results of such systems based on unsupervised learning.[40] Human intervention is nonetheless required to verify whether outputs are performing appropriately or accurately. It can be difficult for developers of unsupervised learning systems to identify how outputs were rendered. When a machine's 'decision-making' or analytical processes are unknown to the public, either through trade secrets or because of challenges with deciphering their logic, these 'black box' decisions could be arbitrary and unfair due to this lack of transparency.[41] When such FRT systems are used in ways that can result in a person's detention and arrest, for example, this may violate a person's right to due process or procedural fairness as protected under the common law and section 7 of the *Charter of Human Rights and Freedoms*, as well as the right to freedom from arbitrary detention under section 9 of the *Charter*.[42]

There are many factors that influence a biometric recognition system's accuracy. When it comes to face recognition, these factors impacting accuracy are present when the system is being developed, as well as when the technology is being used:

- The algorithms used;
- The training datasets used;
- The number and quality of photos used for training, watchlists, and photos taken for comparison;
- Whether composite or artist sketches of images are used in watchlists;
- Whether face recognition is relying on 2D or 3D imagery;
- The presence of facial obstruction or occlusion;
- Whether FRT is used in a live setting or on static images;
- Camera quality and age;
- Environmental factors, including lighting and weather;
- The presence of duplicate images and certain facial images that tend to match with many others;
- Minimum and maximum accuracy thresholds for the production of matches;

- Spoofing, or a person's intentional attempts to disguise their face to look like someone else.[43]

Indeed, a system's training datasets and algorithms greatly affect its outputs, biases, and accuracy rates.[44] This is related to the fact that data itself is never neutral.[45] There are biases built into what data is collected, why it is collected, the kind of data collected, how it is formatted and stored, and other terms of its creation and use. In a similar vein, neither are algorithms neutral.[46] They reveal and replicate the values and biases of their creators and developers. This helps dispel the fallacy or myth that mathematical processes can be more trustworthy or less biased than human decisions simply because they are mathematical.[47] The belief that mathematical processes are objective or free from bias is itself a type of bias that shapes people – from a system's developers to decision-makers like judges to public safety actors. However, it is critical to understand that built into all AI or automated recommendation systems are the biases and values of their creators, which can recreate and exacerbate longstanding power imbalances and inequities in society,[48] including but not limited to the fact that Black and Indigenous people face higher rates of being stopped and searched by public safety actors than people from other racial backgrounds in Canada.[49]

4.1.1 Accuracy Issues and Other Considerations Regarding the Use of FRT

On top of this, there is mounting evidence that the matches provided by FRT systems have accuracy problems that disproportionately impact certain equity-deserving communities. The studies completed to date have largely occurred in the U.S. and in the UK, but are also very much relevant in the Canadian context. For example, a systematic review from 2020 found that FRT can be very error-prone for various reasons related to the factors already mentioned (e.g., image obstruction, facial aging, combining recognition tactics, lack of multiple images featuring individuals).[50] A lack of three dimensional facial scans also means that 3D facial recognition performance remains "very critical and unreliable."[51] Further, the systematic review also found that facial recognition in live settings is also currently under-studied and also remains unreliable for reasons related to image blurring, low-resolution, and parts of images appearing as block artifacts, as well as when faces involve variable poses. Nearly 200 commercial FRT systems analyzed in 2019 by the U.S. National Institute of Standards and Technology (NIST) demonstrated that the technology has discriminatory effects on women, Black, East Asian, and Indigenous peoples.[52] That study revealed that the algorithms analyzed were 10 to 100 times more likely to provide false positives in the one-to-one matching context for Asian and Black people compared to white people.

Research also demonstrates that FRT systems can reproduce long-standing biases and have discriminatory impacts on certain equity-deserving groups related to accuracy rates. This is particularly the case when data-driven systems are relied upon where communities have historically been subject to over-policing.[53] Additionally, foundational work by computer scientists Joy Buolamwini and Timnit Gebru reveals that numerous commonly used commercial gender classification algorithms (including those provided by IBM and Microsoft) performed best on people with lighter skin and on men.[54] There are risks that FRT will fail to recognize certain parliamentarians as *humans*, particularly those who are Black.[55] Amazon's FRT system Rekognition was found in 2018 as misidentifying members of U.S.

Congress who are people of colour through false matches of people depicted in mugshot images.[56] FRT is also known to misidentify gender non-conforming people such as trans and non-binary people.[57] While there have been few studies on the topic, it would be logical that FRT would also have higher mis-identification rates for people with physical disabilities. The implication of such bias and accuracy issues is explained further in **Sections 5.3**, **6.1**, and **6.3**.

Two prominent studies on the use of real-time FRT for public safety provide an example of some of the other considerations that ought to guide any deployment of the technology.[58] The first such study was undertaken in 2018 by Bethan Davies, Martin Innes, and Andrew Dawson of Cardiff University on the use of FRT by the South Wales Police on a trial basis. The second study, mentioned earlier in this section, was undertaken by University of Essex researchers to examine the use of FRT by the London Metropolitan Police.

The first practical lesson that can be taken from these studies is that significant resources are required for implementing face recognition systems. FRT is expensive to implement and could cost hundreds of thousands of dollars, if not millions, depending on the services, software, and hardware procured. For example, when the South Wales Police used FRT, the police force needed to spend considerable amounts on cameras that were recommended by the company they worked with for these services. They ended up spending £67,000 (approximately $110,000 CAD) on 14 cameras. They ultimately needed to replace all 14 cameras due to a manufacturing error, but fell within a warranty period allowing them to be replaced by the provider. The cameras purchased nonetheless performed poorly in low light conditions, and there were talks of replacing them with better quality and more expensive ones. As Davies, Innes, and Dawson conclude, the "evidence generated by this research is that the overall performance of the system involves a number of overt (costs of purchasing and replacing equipment) and more 'hidden' costs (upgrading the quality of custody images [used for watchlists] and how they are taken)."[59]

The South Wales Police also ultimately faced a protracted legal battle regarding their use of FRT. If FRT were to be used in the Canadian federal parliamentary context, resources may be required to respond to legal claims given the legal and human rights risks posed by the technology. Funding could also need to be allocated for public consultations, as well as initial and regular auditing of the technology if the technology were to be used — examples of some of the costs related to a few key considerations that can be gleaned from this report regarding the potential use of FRT.

Research by Davies, Innes, and Dawson, as well as Fussey and Murray, also demonstrates that FRT is by no means 'plug and play' technology. Technologies deployed by public safety actors are often framed as 'magic bullets' to help solve legitimate occupational and organizational issues, yet there is often a significant difference between how the technology is perceived and how it functions when used on the job.[60] More than this, significant human resources and training are required for the use of FRT. The South Wales Police, unlike the London Metropolitan Police, explicitly disclosed to the public that FRT was being used and also engaged in public awareness campaigns regarding its deployment. In the parliamentary context, many decisions regarding the potential deployment of FRT would also be needed, such as the criteria for who goes on watchlists, strategies for deploying tech in certain locations, handling

and assessing data, and policies for the PPS's activities based on validated matches, among numerous other considerations.[61] Technical training would also be needed for staff members regarding the handling and operation of the technology and, importantly, for addressing the discriminatory and potentially rights-infringing impacts of the technology.

Training and explicit, written policies would also be needed for handling particularly sensitive situations, such as an FRT system resulting in the recognition or potentially misrecognition of people who are engaging in lawful political free expression, who are in mental health crises, or who are unhoused, as well as children. For example, Fussey and Murray observed that the London Metropolitan Police's use of FRT resulted in the questioning of a 14-year-old child.[62] Police began questioning this child despite the fact that an operator later assessed the alleged match as inaccurate. The child was a "uniformed schoolboy" who "was stopped and surrounded by five plainclothes officers" around 20 metres from the van used for face recognition.[63] The police engaged in an identity check, realized that they had the wrong person, and the altercation was followed by "conflict on the streets with an adult female shouting at the officers and complaining about the police engaging with children in this manner."[64]

PPS is not immune from the possibility of its team members engaging in such treatment of vulnerable or minority communities, which could be exacerbated by the use of technology such as FRT. For example, a group of Black human rights, labour, and youth groups were attending an event called Black Voices on Parliament Hill with Cabinet ministers in 2019.[65] The visitors stated that a government employee complained about them to PPS and referred to them as "dark-skinned people." A PPS staff member allegedly asked the group to leave despite them having the permission and valid passes to be there. The Speaker of the House of Commons later apologized for such racial profiling and the Prime Minister ultimately issued an apology while also launching an investigation into the incident.[66]

Relatedly, an Indigenous Member of Parliament, Mumilaaq Qaqqaq, stated that she was regularly stopped and questioned by PPS staff members, and had experienced racial profiling since being elected in 2019.[67] She told news media that she "never felt safe", that security personnel would sometimes jog after her in the hallways when she entered buildings, and that every time she walked on the House of Commons grounds, she felt reminded that she didn't belong there.[68] In 2021, she ultimately decided not to run for re-election.

As explained in **Sections 5.3** and **6.3**, technology such as FRT can perpetuate and exacerbate such long-standing inequities in communities and the contexts in which the technology is used, while also facilitating the infringement of people's *Charter* rights with decreased human intervention. Numerous measures could be taken to address the risks of FRT, as outlined throughout this report in the parliamentary context. For example, it would be important to have a human assess and validate any matches provided by an FRT system before action is taken based on that match, such as detaining someone or limiting their entry into a geographic area. This is because when FRT systems are used in ways that can result in a person's detention and arrest, this may violate a person's right to due process or procedural fairness as protected under the common law and the *Charter of Human Rights and Freedoms*, as well as the right to freedom from arbitrary detention.[69] These issues should be tackled and addressed prior to the use of this technology; and, if the technology is nonetheless used after in-depth privacy and human rights analyses, the technology's risks would need to be addressed and mitigated throughout its use.

4.2 Contextualizing FRT

Over the years, there have been significant changes in national and international security impacting public safety and security practices.[70] These changes have been facilitated by data-driven technologies such as artificial intelligence and other analytics software. They also factor into larger trends aimed at preventing wrongdoing and detecting security risks through advanced data gathering and processing systems. Research on data collection technologies and the ways in which they have shaped public safety and security practices, as well as their consequences, have been well-documented for some time — including their roles in expanding state surveillance.[71] More recently, such trends have accelerated while technological advancements have spurred on increased uptake of potentially intrusive technology.[72]

In tandem, public safety and security norms have shifted from a reactive or preventive logic to one where pre-emption is a primary goal, enabled by technology.[73] This has drawn crime and security policymaking discussions closer to the concept of 'pre-crime' which "shifts the temporal perspective to anticipate and forestall that which has not yet occurred, and may never do so."[74] Public safety actors such as police agencies in the United States have experimented with — and many continue to use — data-driven technologies that claim to 'predict' crime within a certain geography,[75] while other systems have been designed to identify individuals suspected to commit future crimes using proprietary algorithms that calculate 'risk' scores.[76] The use of such technologies has drawn significant criticism by experts and community groups for their wide-ranging sociotechnical and political consequences, including their potential to violate human rights and civil liberties, with members of vulnerable and marginalized communities facing particular concerns as also discussed in various sections of this report.[77]

Although many of these discussions often take place within the U.S. and EU contexts, reports reveal that Canadian public safety and security agencies are increasingly deploying, using, or planning on procuring such technologies.[78] The Vancouver Police Department is currently using data-driven technologies to identify the likelihood of crimes taking place within particular neighbourhoods;[79] while in Saskatchewan, police are analyzing data to identify individuals who may be involved in illegal activity.[80] Against this backdrop of increasing desire for security, coupled with the push to achieve greater efficiency and effectiveness,[81] there is an ever-increasing accumulation of security products by state actors that seek to predict wrongdoing,[82] including face recognition technology.

The events of 9/11 have catalyzed the development and use of FRT in particular, which has been perceived as a solution to the "unidentifiable" enemy.[83] Indeed, since around 2004, FRT has been used at Canada's border with a view to prevent passport fraud.[84] A handful of police services in Canada have also particularly begun using or attempting to use FRT over the past several years, with many agencies lacking robust policies on its use,[85] and with significant gaps in privacy and human rights laws concerning the collection of highly sensitive biometric information such as facial images for automated processing.[86]

4.3 FRT Potential Use Cases in the Parliamentary Context

There are numerous publicly-known and obvious physical security and surveillance measures in place in the parliamentary context, such as the use of CCTV and visitor screening. More specifically, news reports indicate that metal detectors were installed at the entrances to the House of Commons gallery in 1982.[87] Non-official vehicles were barred from entering Parliament Hill in 1997, while metal bollards were installed at the Hill's three main gates for vehicle access.[88] While it was still in charge of security for the physical grounds of Parliament Hill as described in **Section 5.1**, the Royal Canadian Mounted Police (RCMP) added 134 CCTV cameras to the existing 50 cameras in 2013 to monitor access to Parliament Hill, as well the exterior of all buildings, pedestrian doors, and areas that allow for the gathering of groups of people.[89] At the time, the RCMP stated that the cameras' logs were kept for 90 days and video feeds for 30 days. The Office of the Privacy Commissioner (OPC) told news media that many of the cameras are monitored round-the-clock and have the ability to record close-up images, as well as panoramic views.[90] After a back and forth with the OPC, which enforces Canada's federal privacy laws, the RCMP agreed to post signs informing the public of the 24-hour video surveillance, given Parliament Hill's role as an important site of political expression for groups across the country. Ongoing renovations for Parliament buildings have also prompted conversations regarding the possible implementation of additional security tactics, tools, and practices.[91]

As an illustrative and purely hypothetical exercise, potential use cases of FRT in the parliamentary context are summarized in Table 1. The term 'restrictive' is used to convey the more limited nature of the deployment of FRT, rather than solely the perceived level of restriction that could be placed on rights.[92] While this is just one way to assess impact, deployment that is 'more restrictive' refers here to the assumption that a smaller number of people could be impacted if FRT were to be deployed as described when it comes to location, timing, and who is targeted by FRT. Conversely, 'least restrictive' assumes that a greater number of people could potentially be impacted if the technology is deployed in such a fashion regarding the location, timing, and those targeted by the use of FRT.

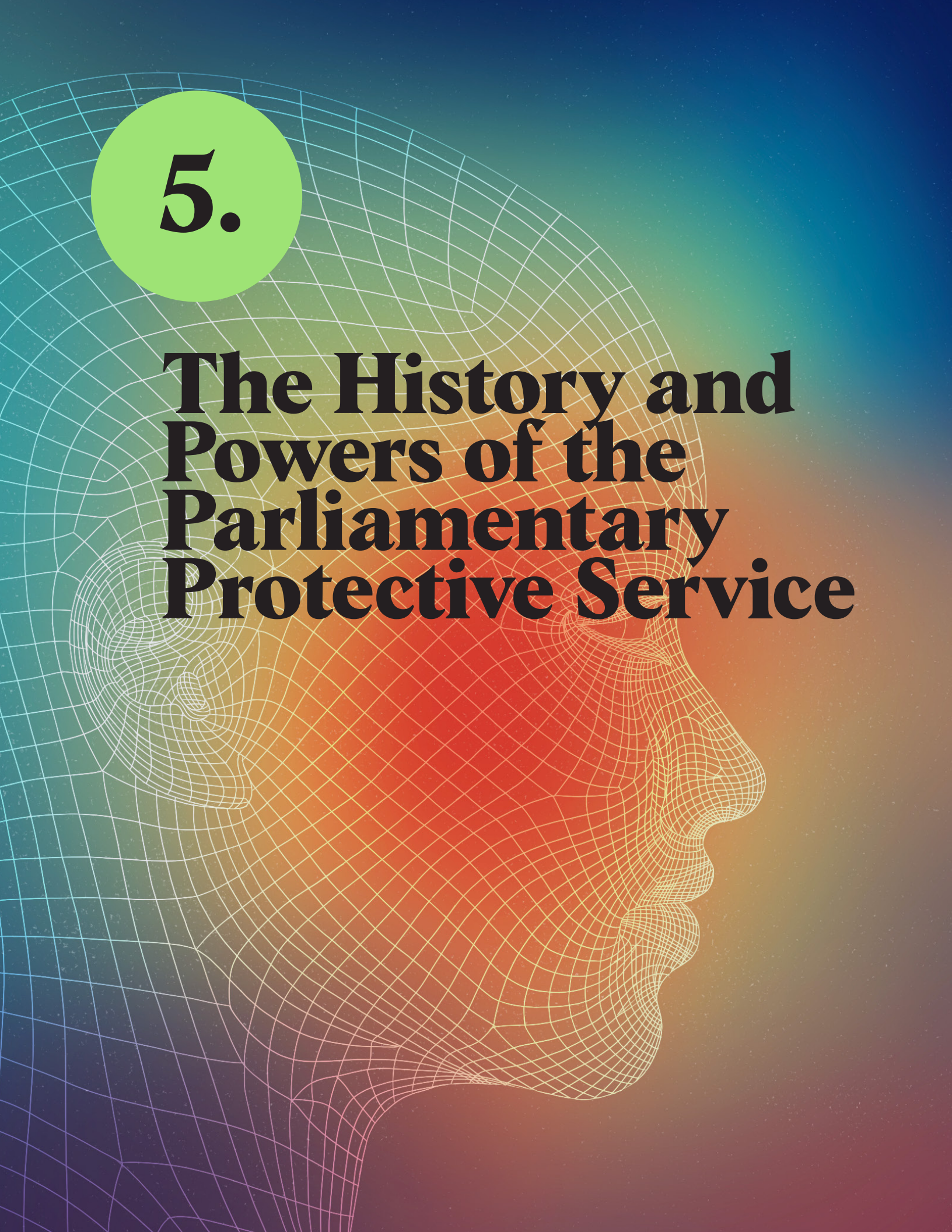
This heuristic is non-exhaustive and these prongs of analysis exist on a spectrum. This information is provided to outline the various hypothetical ways the technology could potentially be used, as each brings different privacy and human rights considerations and risks. Related analysis in the UK includes the Surveillance Camera Code of Practice, which requires determining the specific problem that needs to be addressed through the use of an intrusive privacy measure, who will be targeted using the measure, why the measure is necessary and proportionate, when it would be used, and where.[93]

Table 1: Potential Use Cases of FRT in the Parliamentary Context – From Most to Least Restrictive Levels of Deployment

	Location of Deployment	Timing of Deployment	Targets of FRT	Purpose and Conditions of Deployment	Notice and Consent Regarding Deployment
Most Restrictive Deployment	Inside Parliament buildings (some or all)	When a specific, time-limited security threat has been identified (e.g., a bomb threat)	PPS and/or domestic or international security partners	Categorization based on 'soft' face-related information only (e.g., person's gender, ethnicity, age, etc.)	Knowingly opted into and revocation of consent is possible for entry into location where FRT is used
↑	At interior entrance of Parliament buildings (some or all)		Parliamentarians (Members of Parliament and Senators), staff, and employees		
Level of Restrictiveness Regarding Deployment	At outdoor entrances of Parliament buildings (some or all)	During a time-limited event at parliamentary precinct and on Parliament Hill		Authentication of known identity through one-to-one comparison	Upon notice of surveillance
↓	Throughout the parliamentary precinct and on Parliament Hill	No time limits; deployed perpetually	All people visiting Parliament		Neither consent nor notice obtained
Least Restrictive Deployment	At perimeter of Parliament Hill		People not yet on Parliament grounds	Unique identification of unknown identity through one-to-many comparison	
	Outside of parliamentary precinct and Parliament Hill				

4.4 Key Considerations

- There are many facial image datasets available that can be used to train an FRT system and employed for watchlists. However, significant legal issues exist around the legality of the construction of such databases. For example, the OPC has concluded that facial image databases and watchlists are to be collected only through lawful means. Aspects of an FRT system such as image quality impact the accuracy of the system.
- FRT systems can reproduce long-standing biases and have discriminatory impacts on certain equity-deserving groups related to accuracy rates — particularly when data-driven systems are relied upon where communities have historically been subject to over-policing.
- Significant resources are required for implementing face recognition systems, including for software, hardware, public consultation, technical and human rights auditing of the technology, training, and potential legal claims arising from the technology's use, among other costs.
- It is important to have a human assess and validate any matches provided by an FRT system before action is taken based on that match, such as detaining someone or limiting their entry into a geographic area, as such actions may implicate the rights to due process or procedural fairness, as well as the right to freedom from arbitrary detention.
- Given that FRT has the ability to facilitate the infringement of people's *Charter* rights with decreased human intervention, the public should be consulted and explicitly notified regarding the potential use of FRT in the parliamentary context.
- These issues should be tackled and addressed prior to the use of this technology; and, if the technology is nonetheless used after in-depth privacy and human rights analyses, the technology's risks should be addressed and mitigated throughout its use.



5.

The History and Powers of the Parliamentary Protective Service

The History and Powers of the Parliamentary Protective Service

5.1 A Brief History of PPS

A brief overview of the history and powers of the Parliamentary Protective Service (PPS) is useful here. The PPS is a relatively new institution, created in 2015 after an armed attacker entered Parliament Hill's Centre Block building and tragically killed a soldier on ceremonial guard.[94] Prior to this, security in the parliamentary context was independently managed by the House of Commons Security Service, the Senate Protective Services, and the Royal Canadian Mounted Police (RCMP).[95]

Security responsibilities prior to the creation of the PPS were complex and described as "operating in silos."[96] The RCMP was responsible for the security of the physical grounds that surround the buildings on Parliament Hill.[97] The Senate Protective Services and the House of Commons Security Service were responsible for the security of the interior of the buildings.[98] These security groups worked with different communication systems, had separate training regimens for staff members, and interactions were limited between the teams.[99] On top of this, the Ottawa Police Service was responsible for responding to alleged unlawful activity on Parliament Hill and had responsibility for the jurisdiction surrounding the area.[100]

After the attack on October 22, 2014, the RCMP temporarily took over operational command of all security on Parliament Hill on February 4, 2015.[101] Reviews by both Parliament and the RCMP[102] recommended the creation of a unified security force.[103] The establishment of the PPS on June 23, 2015 therefore filled a gap by providing physical security services in a more integrated fashion.

5.2 Shared Responsibilities for Physical Security in the Parliamentary Context

5.2.1 The Sources of the PPS's Powers and the PPS's Mandate

The PPS was established by the *Parliament of Canada Act* (the *Act*).[104] A memorandum of understanding (MOU) was signed pursuant to section 79.55 of the *Act* to have the RCMP provide physical security services through the PPS.[105] The MOU provides useful clarifications given that changes to the governance and operations of security in the parliamentary context were implemented very rapidly after the attack in late October 2014.[106]

The PPS was established to provide physical security on Parliament Hill and the parliamentary precinct;[107] and comprises an amalgamation of the Senate Protective Services, the House of Commons Security Services, and the RCMP.[108]

The PPS's mandate is broad. The *Act* requires the PPS to provide physical security in the Parliamentary precinct and on the grounds of Parliament Hill. Section 3 of the MOU further defines the PPS's mandate as including the "physical security of Parliament, its premises, Parliamentarians, Parliamentary Staff, and guests of Parliament."[109]

Importantly, the PPS is not law enforcement, but has the ability to detain for arrest by law enforcement by virtue of its mandate to ensure physical security.[110] The MOU also states that the PPS will refer "allegations and complaints of criminal activity" to "appropriate police officers outside the Parliamentary Protective Service."[111] The MOU states that "subsequent policing activities will follow established protocols consistent with parliamentary privileges and traditions."[112] It could be presumed that the subsequent policing activities referred to here generally capture the actions of police of jurisdiction, such as the RCMP or the Ottawa Police Service.

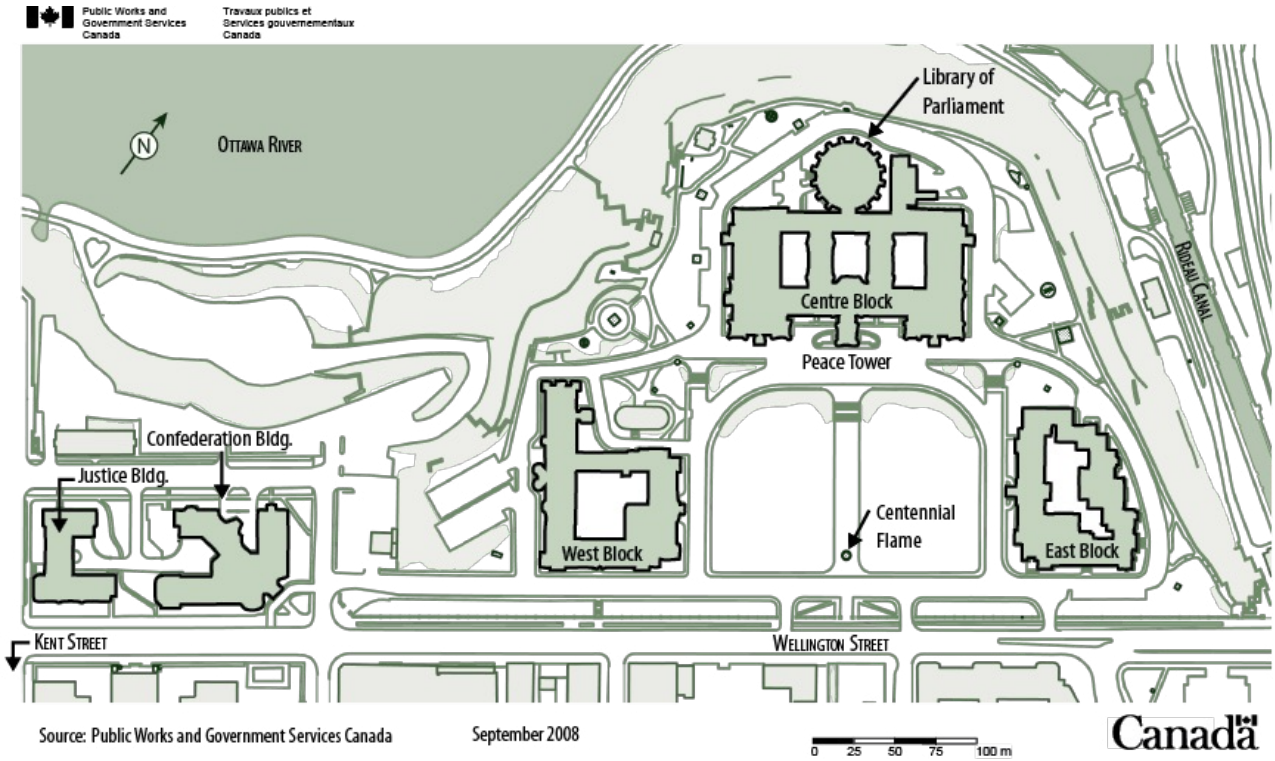
The *Act* sets out the geographic areas relevant in the parliamentary context. Section 79.51 of the *Act* defines "parliamentary precinct" as the premises or any part of the premises (except the constituency offices of members of Parliament) that are used by the following entities or individuals, or their officers or staff:

a. the Senate, House of Commons, Library of Parliament or Parliamentary committees;
b. members of the Senate or the House of Commons who are carrying out their parliamentary functions;
c. the Senate Ethics Officer or the Conflict of Interest and Ethics Commissioner;
d. the Service; or
e. the Parliamentary Budget Officer.

The premises must be designated in writing by the Speakers of the Senate or the House of Commons.[113] The Speakers can also alter what geographic areas and buildings are included in the meaning of "parliamentary precinct" so long as they advise and consult with the PPS's Director regarding these changes.[114]

"Parliament Hill" is defined as the grounds in the City of Ottawa bounded by Wellington Street, the Rideau Canal, the Ottawa River, and Kent Street.[115] A map of Parliament Hill can be viewed below.

Figure 1: A Map of Parliament Hill[116]



Part of the PPS's mandate includes certain considerations and limitations. Importantly, the MOU requires the PPS to "be sensitive and responsive to, and act in accordance with, the privileges, rights, immunities and powers of the Senate and the House of Commons and their Members", which are concepts that will be explained and analyzed in **Section 5.3**.[117] The PPS must also allow other branches of the RCMP (such as the Prime Minister's Protective Detail) to carry out their functions within the parliamentary precinct.[118] The PPS and its staff members must also "have due regard to the need to ensure reasonable access to the Parliamentary precinct and the grounds of Parliament Hill."[119]

Paragraph 3 of the MOU states that the definition of physical security "excludes IM/IT infrastructure and IT security, including the sharing and protection of data." The issue of responsibility for the security of digital infrastructure is relevant for any use of FRT in the parliamentary context because using the technology would involve the collection, processing, and potential sharing of data such as facial images, facial templates, and potentially information about people's travel locations and patterns, all of which is highly sensitive in nature. The PPS has stated to us in the course of our research that responsibility for IM/IT infrastructure and IT security is a shared responsibility with the House of Commons, and that the PPS has its own data classification system and is actively educating its staff members on criteria used for this classification. The PPS has also informed us that it has developed an Information Management policy, Personal Information Handling procedures and a methodology for Personal Information Assessments.

5.2.2 The Key Players Regarding Physical Security in the Parliamentary Context

Under the *Act*, both of the Speakers of the Senate and the House of Commons are responsible for "all matters with respect to physical security throughout the parliamentary precinct and Parliament Hill."[120] The law states that the Speakers are ultimately "responsible for [the PPS]" as "custodians of the powers, privileges, rights and immunities of their respective and of the members of those Houses".[121] Section 7a of the MOU states that the Speakers of the Senate and the House of Commons have ultimate authority for the security of the *parliamentary precinct*.[122] However, this provision of the MOU is silent on whether the Speakers have authority for the security of *Parliament Hill*. Nonetheless, the Speakers are also required to "set general policy, including annual objectives, priorities and goals" related to the security of both the parliamentary precinct and Parliament Hill, in consultation with the PPS's Director.[123]

While the RCMP remains distinct from PPS, the MOU nonetheless provides the RCMP with an important role in the provision of physical security in the parliamentary context. Indeed, the MOU was signed by the Speaker of the Senate, the Speaker of the House of Commons, and the Minister of Public Safety as an arrangement to have the RCMP provide physical security services throughout the parliamentary precinct and Parliament Hill."[124] Further, the MOU states that the RCMP must "lead integrated security operations throughout the parliamentary precinct *and* on the grounds of Parliament Hill."[125] The Director of the PPS must also be a member of the RCMP;[126] and is appointed through a consensus-based process by the RCMP Commissioner, the Speaker of the Senate and the Speaker of the House of Commons.[127] The Commissioner of the RCMP

reports to the Minister of Public Safety and is responsible for the control and management of the RCMP.[128] Members of the PPS may include members of the RCMP,[129] but the PPS's Director is currently the only staff member who is also a member of the RCMP.

5.3 The Legal Nature of the PPS and the Role of Parliamentary Privilege

A very important concept for analysis in this report is parliamentary privilege. The Supreme Court of Canada has defined parliamentary privilege as the sum of the privileges, immunities from the law, and powers enjoyed by the Senate, the House of Commons, and provincial legislative assemblies, and by each member individually necessary to do their legislative work.[130] The concept is in use because settlers from the United Kingdom imported the Westminster system of governance for the federal government during the founding of Canada as a country.[131] The doctrine of the separation of powers between the legislative, executive, and judicial branches of the state was also imported to Canada along with the Westminster governance system. While the legislative branch can claim immunity from the application of the law through parliamentary privilege, the executive and judicial branches cannot claim this privilege. Parliamentary privileges can be claimed collectively by each of the two Houses (the Senate and the House of Commons) or they can be claimed by members of the Houses individually.[132]

In short, when an activity is protected by parliamentary privilege, courts cannot review its exercise or compliance with the *Constitution Act* (including the *Canadian Charter of Rights and Freedoms*) and other statutes.[133] However, courts may review whether the claimed privilege's existence is necessary for the two Houses and its members to "carry out their parliamentary functions of deliberating, legislating and holding the government to account, without interference from the executive or the court."[134] The immunity from judicial review afforded by parliamentary privilege is particularly significant for people whose rights may be impacted by its exercise. For example, visitors to Parliament Hill and the parliamentary precinct do not benefit from parliamentary privilege and may be harmed by the exercise of privileged activities that could infringe their rights under laws such as the *Charter* and the *Privacy Act*.[135]

5.3.1 Parliamentary Privilege and Parliamentary Security

Our analysis finds that parliamentary privilege is a crucial concept in the context of the PPS's work because it can both enable and limit its activities. The PPS can claim that parliamentary privilege enables much of their activity by virtue of sections 79.53(1) and 79.52(2) of the *Parliament of Canada Act*, which gives the Speakers of the Senate and the House of Commons ultimate responsibility for the physical security of the parliamentary precinct and Parliament Hill, as well as for the PPS.[136]

One way that the PPS could rely on parliamentary privilege to shield its activities from judicial review is through the recognized privilege of the Senate and House of Commons to manage their own internal affairs.[137] The privilege of the two Houses to manage their own internal affairs has been recognized in relation to the decisions of the House of Commons' Board of Internal Economy and other types of activities, and could include some aspects of security operations.[138] However, the privilege for the Senate and House of Commons to manage their internal affairs is not absolute and

courts have limited its scope.[139] For example, in *Canada v Vaid*, the Supreme Court of Canada found that the relationship between Parliament and its employees was subject to and reviewable under the *Canadian Human Rights Act* in the context of a claim of discrimination.[140]

The PPS could also attempt to rely on the House of Commons' privilege to exclude strangers from legislative precincts, with a view to justify its use of certain physical security and surveillance measures. In the past, this privilege has been called upon to shield from judicial review decisions to exclude journalists with cameras from House of Commons proceedings[141] and to deny entry to a delegation of Sikh men carrying their kirpans.[142] Legislatures have also used this privilege to place bans on visitors who have caused past disruptions within a legislative precinct. In one case at Queen's Park, the Legislative Assembly of Ontario placed a ban on protestors who had thrown blood-coloured paint to the walls of the legislative building.[143] The Ontario Superior Court of Justice ruled in that case that the legislative precinct, and therefore, the legislature's authority to exclude strangers without judicial review, extended beyond the legislative building.[144]

However, our analysis suggests that the PPS's activities can also be limited by parliamentary privilege. For example, the PPS could engage in activities that violate or at the very least challenge parliamentary privilege for an individual member or possibly one of the Houses as a collective. Indeed, both the *Parliament of Canada Act* and the MOU stipulate that the PPS cannot limit the powers, privileges, rights, and immunities of the Senate and the House of Commons.[145] This is not a hypothetical concern. A parliamentarian testified in 2017 that he was prohibited from entering Parliament because an escort of the Prime Minister's motorcade was arriving and monopolizing security services. As a result of the delay, the parliamentarian and his colleague arrived late to the vote and were unable to exercise their functions as members of the House. He alleged that this was a breach of parliamentary privilege.[146] Similarly, a researcher for the Standing Committee on Procedure and House Affairs found in 2017 that there had been seven instances "involving members being impeded or delayed from accessing Parliament Hill and the parliamentary precinct freely" due to the use of security measures by PPS personnel, with the result that the members of the House of Commons missed votes.[147] It is therefore clear that the use of certain security measures in the parliamentary context must be examined in light of parliamentary privilege.[148]

5.3.2 Face Recognition Technology and Parliamentary Privilege

To claim that the use of surveillance measures such as FRT is shielded by parliamentary privilege, it may be possible to argue that the technology is an extension of physical security practices in place that generally help the legislature identify people who ought not to enter Parliament Hill and/or the parliamentary precinct. The idea would be that the technology would help the Senate and the House of Commons, as well as its individual members, exercise their functions by rooting out individuals who threaten physical security even before they engage in wrongdoing through the rapid identification of such individuals on an automated basis. This practice would aim to prevent an unwanted person from entering the protected parliamentary area or lead to them being apprehended for removal or arrest. One could also hope that the use of FRT would improve the ease of access to Parliament for Senate and House of Commons members, as well as their staff, or

to be used for authentication purposes with digital access passes. The use of FRT could be used with the goal of aiming to reduce the amount of parliamentarians' faces that must be memorized by security staff in the parliamentary context.

However, the reasons for FRT's appeal also relate to many of its concerns for parliamentarians. This is because the use of FRT authentication and the unique identification of individuals is fundamentally different than relying on humans to do such activities. As explained in **Section 4.1**, FRT is very powerful in the way it enables the rapid capture of a large amount facial images for analysis, as well as the rapid comparison of such faces against either a particular stored facial template or one or more watchlists. The speed at which FRT can be used to identify people is also an indication of how quickly the technology may prevent a parliamentarian from accessing the parliamentary precinct and Parliament Hill; how quickly it may misrecognize a parliamentarian; or how quickly it can be used to profile parliamentarians and track their travel history. Algorithmic and automated biometric recognition technology such as FRT can facilitate surveillance of the human body at increased speed and scale. Such technology also learns from and reproduces human biases. The following analysis makes clear that the use of technology such as FRT to augment human decision-making processes for physical security could pose significant risks to parliamentary privilege for parliamentarians.

In particular, the use of FRT may have discriminatory impacts on parliamentarians and their staff. More specifically, as described in **Section 4**, the technology is known to have higher inaccuracy rates for equity-deserving and minority populations. A major problem here would be the exercise of parliamentary privilege, ostensibly in the collective's interest, but with arbitrary and discriminatory impacts on individual parliamentarians and their staff. If certain parliamentarians or their staff members are either not recognized as human or are misrecognized as someone else by FRT, then the technology could also prevent parliamentarians from entering premises (even if temporarily) and could ultimately impede or prevent them from exercising their functions and duties with the independence and dignity they deserve.

In a recent report of the House of Commons, one parliamentarian suggested that parliamentary privilege should be seen as a way to protect parliamentary minorities.[149] Parliamentary minorities are most likely to be negatively impacted by surveillance technologies. These could be demographic or political minorities. For example, parliamentarians from racialized, religious, or language minority groups may have more to lose — in terms of the freedom of movement, expression, and association — from the use of physical security and surveillance measures such as the deployment of FRT.[150] Similarly, political minorities, such as members of opposition or smaller parties, may express more resistance to the use of such a system throughout the parliamentary precinct and on Parliament Hill. Given the previous claims of racial profiling by some minority parliamentarians related to the PPS's security personnel, the possibility of perpetuating and potentially automating such treatment should be a primary consideration in all decisions regarding the potential deployment of FRT and similar technology.[151]

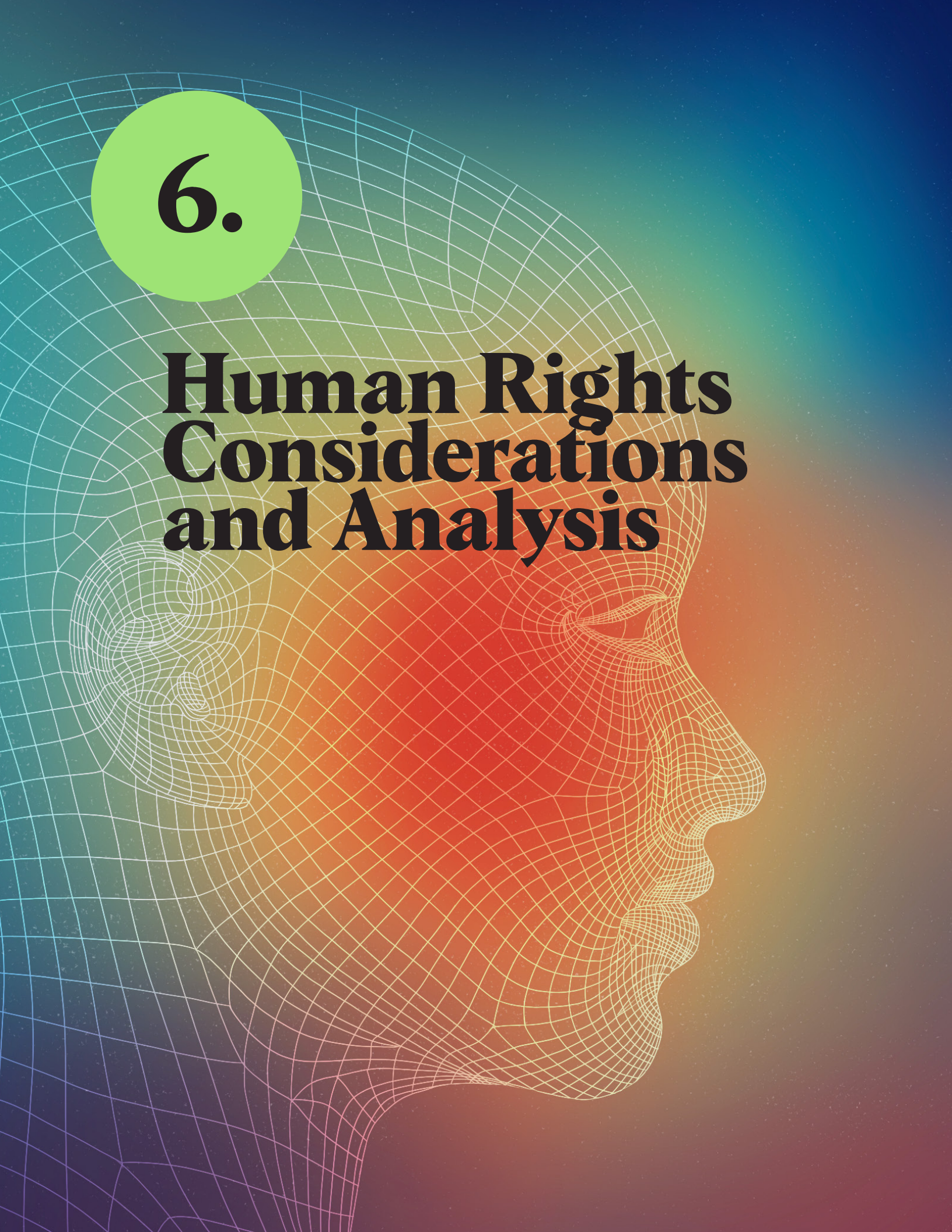
Even if the technology's discriminatory effects are addressed, the technology could potentially still disrupt parliamentarians' ability to exercise their duties with a certain level of privacy and independence from the executive. If FRT is used at multiple

entrances and exits of indoor and/or outdoor spaces, it is possible that the whereabouts and travel patterns of parliamentarians, their staff members, and their invited visitors could be known and tracked by the technology. This would be the case if the technology is used only on such people for authentication purposes — for example, where the system captures only individuals' faces and compares them to a stored facial template on an RFID device.[152] FRT could also track the travel patterns of parliamentarians, their staff members, and their invited visitors if all people's faces are scanned by the technology for unique identification and compared against one or more watchlists.[153] In the event that such information was shared with entities that the PPS has data-sharing relationships with, such as the RCMP that fall under the executive, it could be challenging to claim that this tracking and data-sharing activity can be shielded from judicial review by being a matter of parliamentary privilege. In addition, this activity may violate the parliamentary privilege of the Senate and the House of Commons each as a collective, as well as their individual members, if such information is used by the executive in a way that interferes with their ability to fulfil their collective and individual functions with dignity, efficiency, and autonomy.

As this analysis makes clear, the potential use of FRT in the parliamentary context is appealing for reasons that relate to the risks it poses to parliamentary privilege. The technology can be used to authenticate and identify people's identities at rapid speed, but can also be used to track travel histories and impede or prevent entry to Parliament Hill and the parliamentary precinct in ways that discriminate against minority populations. The potential sharing of this information with the executive branch could also challenge the ability for the legislature to act independently from the executive. The potential sharing of this information with the executive branch could also challenge the ability for Parliament to act independently from the executive. Parliament may wish to build in codified guardrails in light of the risks posed by security measures such as FRT in order to ensure that its independence from the executive is not jeopardized.

5.4 Key Considerations

- FRT could potentially be used to authenticate and uniquely identify people's identities at rapid speed, but can also be used to track travel histories and prevent entry to Parliament Hill and the parliamentary precinct in ways that potentially discriminate against minority populations.
- The potential use of FRT could disrupt parliamentarians' ability to exercise their duties with a certain level of privacy and independence from the executive if data is shared.
- To ensure that their independence from the executive is not jeopardized, parliamentarians may wish to build in codified guardrails regarding the collection and automated processing of facial images by the PPS.



6.

Human Rights Considerations and Analysis

Human Rights Considerations and Analysis

6.1 The Right to Privacy

Privacy and data protection rights must be prioritized and protected prior to any use of FRT and, if it is implemented, throughout the entirety of its use. Privacy can be conceived in various ways, but common to many definitions of privacy is a person's or community's ability to determine what information is known about them, who knows this information, and how this information is used.[154] Such informational privacy or self-determination is part of the bedrock of fundamental rights in Canada and other democratic countries around the world. In the words of the Office of the Privacy Commissioner (OPC), privacy is "vital to dignity, autonomy, personal growth and the free and open participation of individuals in democratic life. When surveillance increases, individuals can be deterred from exercising these rights and freedoms."[155]

Indeed, Canada is a signatory to the *International Covenant on Civil and Political Rights* (ICCPR). Section 17 of the ICCPR prohibits arbitrary and unlawful interferences with a person's privacy, and unlawful attacks on honour and reputation.[156] The protection of privacy enables the protection of other related rights such as the right to engage in free expression, the freedom of assembly, and the right to substantive equality.[157] Privacy has quasi-constitutional status in Canada, and the OPC, which is responsible for enforcing the *Privacy Act*, has concluded that the "freedom to live and develop free from surveillance is a fundamental human right."[158]

This section involves analysis of two areas of law. The first area of law includes federal privacy law requirements for 'government institutions' such as those stipulated by *Privacy Act*,[159] the principles of necessity and proportionality, and related impact assessments. The second area of law includes section 8 of the *Charter of Rights and Freedoms*, which is a source of privacy protection from state intrusion by providing all people the right to be secure against unreasonable search and seizure. The *Charter* is relevant in this context because compliance with privacy statutes may not necessarily cure any legal defect that can exist under the *Charter*.[160] Further, limitations of any *Charter* right must be prescribed by law in order to be saved under section 1.[161] As this section shows, there are considerable privacy risks raised by the use of FRT under both areas of law, which ought to be considered by decision-makers at the PPS, as well as parliamentarians involved in authorizing its procurement or use.

Despite not being subject to the *Privacy Act* as a part of the legislative branch, we would encourage the PPS to consider adhering to privacy best practices and federal legal requirements regarding the technology's potential use so that its measures are in line with that of other government institutions and as a matter of the rule of law.[162] More than this, the PPS may wish to set an example for other institutions in its commitment to protecting privacy while achieving physical security, openness, and democratic accessibility for the parliamentary precinct and Parliament Hill.

6.1.1 Federal Privacy Law and Policy Requirements Regarding Facial Information

The privacy principles of necessity, proportionality, and their related considerations ought to inform the potential collection and processing of facial information through FRT in the parliamentary context. These principles "ensure that privacy-invasive practices are carried out for a sufficiently important objective, and that they are narrowly tailored so as not to intrude on privacy rights more than is necessary."[163] These principles inform the OPC's examination of alleged violations of *Privacy Act* provisions such as section 4, which requires government institutions to collect personal information only when it relates directly to an operating program or activity of that institution.[164]

The PPS is not a law enforcement entity, but common to the PPS and law enforcement is the mandate to ensure public safety. In its guidance document to law enforcement regarding FRT, the OPC provides the helpful reminder that rights are not absolute, yet neither can the pursuit of public safety justify any form of rights violation.[165] And similar to law enforcement, the PPS also has an interest in using privacy-invasive practices only when they are justifiable in a free and democratic society.[166]

The OPC's guidance on the use of FRT in a law enforcement context provides many other lessons regarding the technology's use for public safety more generally, including in the parliamentary context. Any government institution wishing to implement FRT must consider whether the collection of personal information facilitated by the use of this technology falls within their legal authority and whether it respects the general rule of law.[167] The OPC's guidance document emerged from the RCMP's use of Clearview AI's FRT software.[168] In February 2021, the OPC concluded that Clearview AI had provided its face-matching services to law enforcement and private companies based on a database of over three billion facial images that it had scraped from the web without the consent of the people depicted.[169] In so doing, these people found themselves in a 24/7 police line-up — amounting to mass surveillance that was a clear violation of PIPEDA, Canada's federal private sector privacy law.[170] After investigating the RCMP's use of Clearview AI, the OPC concluded that government institutions cannot collect personal information from a third party if the information was collected unlawfully.[171] The OPC concluded that section 4 of the *Privacy Act* requires consideration of whether information that is used for face recognition was collected unlawfully and respects the general rule of law. In short, government institutions cannot relieve themselves of responsibility under the *Privacy Act* by collecting and using information that has already been collected if the initial collection of that information is unlawful.

As part of the principles of necessity and proportionality, the OPC has laid out four considerations — necessity, effectiveness, minimal impairment, and proportionality — that ought to inform any decision to use or continue using privacy-intrusive measures such as FRT.[172] Rolled into the following four-step analysis are relevant sections of the *Privacy Act* that align with and are animated by this four-prong analysis, along with the role of related impact assessments.

Necessity. The first prong of this analysis is necessity. The threshold for necessity is high. The overarching question that should be asked here is whether the measure is reasonably necessary to meet a specific need or objective.[173] The broader a problem is framed, the more difficult it is to claim that

the mass collection of personal information is necessary to address that problem.[174] A broad mandate to prevent or deter wrongdoing or crime has historically not given institutions the power to monitor and record the activities of vast numbers of law-abiding people, including the power to monitor whether they might do something wrong.[175]

If the problem is specific enough, there must also be consideration regarding whether the proposed measure is essential for satisfying that need. Necessary is a higher standard than useful.[176] A system that collects and analyzes biometric information should not be adopted simply because it is useful, convenient, or cost-effective.[177] The need or objective for that measure should be pressing and substantial in nature, and must be demonstrable through evidence.[178] The personal information collected should not be overbroad, and instead should be tailored and necessary to meet the specific goal in question.[179]

In addition, facial images are "highly sensitive" biometric information that warrant a higher standard of protection than other forms of personal information.[180] The OPC has also concluded that having a broad general public safety objective does not justify the use of intrusive technology such as FRT.[181] The use of FRT for face-matching raises privacy concerns, particularly where there may be inadequate laws for fundamental decisions that shape the collection and impact of processing facial information through automated means, as is the case in Canada.[182]

Effectiveness. Flowing logically from the first prong, the second consideration that ought to inform any government institution's use of FRT is whether the measure will be effective in serving the purpose of the objective. Robust evidence needs to be produced to demonstrate that a particular proposed measure will address the institution's specific need.[183] If an institution fails to confirm why the collection of certain information meets a certain need, then the OPC would not be able to conclude that the collection relates directly to an identified and specific program or activity.[184] At this stage, the reliability and accuracy of the measure in question will be considered.[185] This relates to section 6(2) of the *Privacy Act*, which requires government institutions to take all reasonable steps to ensure that the personal information that is used for an administrative purpose by the institution is accurate, up-to-date, and as complete as possible.[186]

Minimal impairment. The third consideration is whether the measure in question extends beyond what is reasonably necessary to achieve the specified objective. This relates to a foundational tenet of the *Privacy Act*, requiring institutions to collect only the minimum amount of personal information necessary for an intended purpose.[187] This is because there must be a "demonstrable need for each piece of personal information collected" in order to carry out the program or activity.[188] Two relevant provisions of the *Privacy Act* also include sections 7 and 8, which require personal information to be used and disclosed for purposes that are consistent with the initial purpose for which it was collected.[189] An institution wishing to implement FRT needs to be able to demonstrate that there are no other less privacy-invasive means that will reasonably achieve the objective.[190] They also need to be able to show evidence as to why these less privacy-invasive measures are not used.[191]

Proportionality. The final prong of analysis involves consideration of proportionality. Here, the question is whether a privacy-intrusive measure that involves an intrusion is proportional to the benefit gained.[192] This involves examination of the privacy impacts

that the measure would have on people based on the details surrounding the use of that measure, the context in which it is used, and the subsequent impacts of this measure on certain groups of people.[193] Institutions must consider whether these privacy intrusions are justified by the benefits of the specific deployment of FRT. Institutions "must be open to the possibility that, in a free and democratic society, a proposed FR system which has a substantial impact on privacy (such as via mass surveillance) may never be proportional to the benefits gained."[194] At the same time, some goals may justify greater privacy intrusions than others. Certain safeguards may be implemented related to the measure that aim to reduce its deleterious impacts.

Public safety actors interested in or already using FRT should conduct relevant impact assessments to identify and address the risks associated with such privacy-intrusive measures. Options include: privacy impact assessments used by the OPC;[195] algorithmic impact assessments used by the Treasury Board Secretariat;[196] or more holistic impact assessments for automated decision-making and recommendation systems used in the public sector that include considerations such as cybersecurity, multiple types of transparency, and the availability of legal recourse for those whose rights are impacted by the technology.[197]

6.1.2 Applying Federal Privacy Law and Policy Requirements to FRT

The following analysis is focused on the hypothetical situation presupposing that FRT would be used for one-to-many comparisons involving all visitors to the parliamentary precinct and Parliament Hill, with any variations to this scenario described as needed. The application of one-to-one FRT on parliamentarians or their staff members for either authentication or identification purposes is dealt with in **Section 5.3**, which examines the relationship between parliamentary privilege and the use of FRT in the parliamentary context.

Assessing the necessity of the use of FRT. The necessity of FRT in the parliamentary context must be considered in light of a specific need or objective. The PPS would understandably first consider pointing to its mandate to justify its use of FRT. As discussed in **Section 5.2**, the PPS's mandate is broad. It exists to provide integrated physical security for the parliamentary precinct and on the grounds of Parliament Hill, which includes the physical security of Parliament, its premises, Parliamentarians, Parliamentary Staff, and the guests of Parliament.[198]

However, it should be noted that institutions have faced challenges when attempting to rely on broad mandates to justify their collection of personal information under the *Privacy Act* when the type or scope of information collected and/or means of collection amounts to an intrusion of privacy. For example, the OPC concluded that the Canada Border Services Agency (CBSA) could not justify its use of CCTV cameras for the broad purpose of "program and professional integrity."[199] This purpose and the amount of employee information captured were found to be overly broad in scope.[200] More than this, the CBSA provided no clear evidence of workplace problems that could justify its use of surveillance cameras to monitor employee conduct and performance.[201] As a result, the OPC concluded that the capture of employees' personal information via CCTV for such a broad range of purposes was not in line with the principle of necessity.

In another example, the OPC concluded that Statistics Canada had not properly defined their public goal or objective with sufficient precision to justify the broad

collection of behavioural, financial, and banking information of thousands of people in Canada.[202] As these conclusions demonstrate, it is not enough to simply describe a measure chosen or to reiterate an institutional mandate to justify a privacy-intrusive measure. The need or objective ought to be pressing and substantial in nature, and institutions must provide evidence that the capture of certain personal information is tailored and necessary to meet the objective in question.

On the topic of FRT specifically, the OPC has concluded that it is "not enough to rely on general public safety objectives" to justify the use of such intrusive technology.[203] This is because collecting highly sensitive personal information such as biometric — and particularly facial — information can only occur if such activity falls within an institution's legal authority and respects the general rule of law.[204] The OPC's investigations into Clearview AI and the RCMP for its use of Clearview AI demonstrate that using facial images without the consent of the people depicted for the deployment of FRT, such as the creation of watchlists, amounts to a form of mass surveillance that is inherently intrusive and contrary to the general rule of law.[205]

The OPC has confirmed that highlighting the usefulness of FRT is also not enough alone to justify its use,[206] particularly considering the technology's potential for surveillance creep, and abuse or misuse. Consider the fact that the RCMP initially defended its use of FRT to support ongoing efforts to identify, locate, and rescue children who had been or are victims of online sexual abuse.[207] However, out of the 521 individual searches conducted by RCMP staff members, only 6% were linked to online child sexual abuse victim identification and 85% of searches were not accounted for at all by the RCMP.[208] As these findings indicate, institutions may attempt to justify the use of privacy-invasive measures such as FRT to address very serious and reprehensible activity, such as child sexual abuse or even terrorism. However, work by cybersecurity and technology expert Bruce Schneier demonstrates that it is not surprising that such extreme activity, while unquestionably deplorable, can be turned to with a view to defend actions that may ultimately weaken and violate the right to privacy and other fundamental freedoms.[209] Allowing the use of highly invasive technology for exceptional edge cases (such as child sexual exploitation) brings with it the risk that it will be used in other broad scenarios — potentially a slippery slope and an example of surveillance creep that ought to be addressed in the parliamentary context.[210]

A final note on necessity is that there are currently no binding laws that specifically govern the collection and automated processing of biometric information such as facial images in Canada, as it occurs through FRT.[211] No judicial authorization is currently needed to collect facial information or conduct searches using FRT. As such, there are currently no firm limits on when institutions may use FRT, under what conditions it can be used, how long they can use it for, who can be placed on watchlists, or other fundamental decisions regarding the technology's use that address its privacy impacts. Use of this technology poses significant risks from a privacy rights perspective, particularly given that there is a lack of clear legal safeguards in Canada regarding its use.

Assessing the effectiveness of FRT. An assessment of the effectiveness of FRT needs to occur as part of the necessary and proportionality analysis that guides the OPC's examination of privacy-intrusive government measures. To demonstrate the

effectiveness of a privacy-intrusive measure, evidence needs to be produced to convey that the action or program will address the institution's specific need. In other words, entities wishing to use FRT should demonstrate that there is a specific problem and show how FRT will address that problem before potential deployment.

Government institutions subject to an investigation by the OPC need to explicitly confirm why the collection of certain information meets a certain need. For example, the OPC investigated Global Affairs Canada (GAC) in 2019 regarding its collection of personal information related to personal travel, which occurred because GAC requested the return of diplomatic passports for certain administrative investigations.[212] Yet GAC failed to demonstrate to the OPC how the collection of such personal travel history was directly related to the investigations they conducted, in contravention of section 4 of the *Privacy Act*. As such, the OPC concluded that GAC did not have the authority to collect that personal information.

Effectiveness is an important line of inquiry that ties closely with the considerations of necessity and minimal impairment. In the context of FRT, any existent accuracy issues call into question the technology's reliability. Accuracy includes the requirement to use personal information that is accurate, updated, and complete pursuant to section 6(2) of the *Privacy Act*.[213] Accuracy also refers to how personal information is used or processed, related to the functioning and outputs of a given measure used such as FRT.[214] As canvassed in **Section 4.1** of this report, there are numerous accuracy and bias-related concerns related to FRT. When such technology is unreliable, it can result in state actions that are arbitrary and challenge the general rule of law. The use of a privacy-invasive measure by the state that results in arbitrary action ultimately makes it more difficult to claim that the government action is both necessary to meet a specific objective and is minimally impairing on privacy and other closely related rights.

Assessing minimal impairment. Whether the use of FRT minimally impairs privacy rights is another important consideration. This prong of analysis relates to the question of whether the collection of certain information is not just potentially useful, but is in fact reasonably necessary for an institution's specific objective. Limiting the collection of information to only what is reasonably necessary is also "an important and a nationally and internationally recognized privacy-risk mitigation measure, especially in the current data-rich environment."[215]

The nature and functioning of FRT, particularly when used for broad-based live comparison, makes it challenging to conclude that using this measure would be minimally impairing on the privacy rights of visitors to the parliamentary precinct and Parliament Hill. This is because FRT is appealing for the very reasons that it poses concerns. It involves the capture of faces, which can easily be done at a distance with no notice to the people whose facial images are collected and compared to watchlists. By design, people's faces are also captured without their consent when live FRT is used. The capture of such biometric information from afar without consent, and potentially without notice, is fundamentally different from the capture of biometric information such as fingerprints, blood, or DNA, which are done with a person's knowledge and consent or at the very least under lawful authority.[216] In this way, FRT is concerning from a human rights perspective because it scans for people who are believed to pose security risks in a given context while doing so in a discreet manner, as well as at enormous

scale and speed in ways that could not have occurred otherwise.

On top of this, the very premise of FRT serves to undermine the personal autonomy of the individual. The Supreme Court of Canada has held in *R v Dyment* that the use of a person's body without their consent to obtain information about them "invades an area of privacy essential to the maintenance of [their] human dignity."[217] In that decision, which involved interpretation of the *Charter*, the Court examined the right to privacy where the police seized a person's blood for investigation without a warrant after it was collected by a doctor for medical purposes only. The Court concluded that the trust and confidence of the public in the administration of medical facilities would be harmed if an easy and informal flow of people's bodily information were allowed between hospitals and agents of the state. Similarly, faces constitute biometric information unique to each person; and facial images can currently be collected without consent and without judicial authorization due to gaps in Canada's legal framework regarding biometric information. It is possible that the potential use of FRT in the parliamentary context, if discovered by the public, would affect the public's trust and confidence that their privacy and other rights are being adequately protected and prioritized by the democratic institutions whose primary purpose is serving them as people — particularly if their facial information is shared freely without consent and in a way that is inconsistent with the purpose for which it was originally collected.

To justify the collection of highly sensitive biometric information such as faces and the templates that can be made of a person's face, there needs to be a demonstrable need to collect and retain each piece of information. Any facial templates collected beyond a demonstrable need should be deleted immediately; and, if stored, should be de-identified to be in line with best practices regarding the storage of biometric information and to reduce the risk of privacy intrusions.[218] Yet, even if facial information is stored in a de-identified manner, the fact that this information can be used to identify a person and track their location is of significant concern from a privacy perspective. Indeed, in *R v Spencer*, the Supreme Court of Canada found that the capture of information by police that identified a person, and revealed their location and intimate personal behaviour, was unlawful.[219] The Court was interpreting the *Charter* in *R v Spencer*, yet this decision nonetheless serves as a reminder that, while this right is not absolute, all people have the right to informational privacy — and anonymity is a foundational aspect of informational privacy. By enabling the identification of people, and tracking their movements and behaviour through the collection of facial information, the use of FRT may extend beyond what is reasonably necessary to achieve a specified objective set out by the PPS in the parliamentary context.

Our research also indicates that there may be alternatives to FRT, such as reliance on staff members to identify people based on a watchlist or monitor for suspicious behaviour. Other alternatives that could be less intrusive include security tactics used for the protection of government buildings not involving biometric information that are in place elsewhere in the world.[220]

Assessing proportionality. FRT raises issues regarding proportionality, particularly when it is used for one-to-many comparisons. To assess whether the use of FRT involves intrusions that are proportional to the benefits of such technology, a fundamental question is what privacy rights ought to look like for people who visit Parliament Hill and the parliamentary precinct.

There are numerous related questions that must be considered. Should people be able to visit Canada's Parliament without fear that their identity could be known, and their locations tracked by agents of the state based on the discreet capture and automated analysis of their facial information? Should only some people have this right? If so, who is less deserving of the ability to visit Parliament free from this fear? On what basis should certain people be subject to such scrutiny in the parliamentary context? What historical information about a person, if any, ought to inform who is subject to this scrutiny — such as information relating to those who have been asked to leave Parliament, people charged with crimes, those convicted of crimes, those on terrorist lists, or otherwise on other watchlists? How accurate are those lists? What role has systemic discrimination played in the creation of those lists? Should current actions, such as potentially carrying a weapon, be enough to trigger such scrutiny? What if carrying an object deemed a weapon is part of a person's religious practices and expression?

How one answers these important questions informs the answer of whether the use of FRT for one-to-many comparisons involves intrusions to privacy that are proportionate to the technology's identified benefits. As the Court concluded in *R v Dyment* about law enforcement, ensuring the physical security of the parliamentary precinct and Parliament Hill is important and beneficent, but "there is danger when this goal is pursued with too much zeal."[221] One key risk is that FRT could be overbroad in the information that it captures, particularly when there are fewer limitations regarding its use in terms of where it is used, the conditions under which it is used, who it may be used on, and for how long. Indeed, the collection of facial information en masse to find those who match with a watchlist or to find a lost child, for example, could be likened to finding a needle in a haystack. The capture of people's facial information in the parliamentary context may also amount to mass surveillance while challenging the right to the presumption of innocence, given that the unlawful bulk collection of facial information without people's consent may mean that people find themselves in a 24/7 police line-up.[222] It is also helpful to remember that the use of intrusive surveillance measures such as FRT may give state actors such as the PPS significant insight into who visits Parliament and their travel patterns. Moreover, the technology can fast-track the ability to limit people's access to one of the country's most important democratic institutions, and with potentially discriminatory effects on equity-deserving minority populations. It may be therefore difficult to conclude that the use of FRT for the benefit of a few is justified by the overbroad collection of personal information that is enabled by this technology, particularly given the technology's potential impact on other rights beyond the right to privacy.

If the technology is nonetheless used, certain decisions can be made that would aim to reduce the risks it poses in terms of privacy rights and other rights protected by the *Charter*. Setting firm policies that reduce how, when, where, and why FRT is used would be a first general set of steps that could be useful in mitigating the technology's risks. These limits include crafting specific, targeted purposes or triggers for its use; temporal limits on its use; limiting its use to the fewest geographic locations or to specific locations; and limiting whose facial images are scanned, compared, and stored.

For example, it is possible that live FRT could pose fewer privacy-related concerns if used for authentication purposes at indoor entrances into buildings with good

lighting and only when the facial images of a smaller, select and fixed group of people are collected, processed, and immediately discarded, such as PPS staff members or parliamentarians who knowingly opt into its use. However, the other concerns raised throughout this report such as parliamentary privilege, as well as accuracy and bias concerns for minority populations, could potentially nonetheless remain in this context.

Further, while this line of thinking is more exploratory, scope or function creep are also important concerns when it comes to the use of FRT to protect parliamentary buildings. It is not difficult to imagine that such technology could initially be used for a narrow and specific purpose in the parliamentary context, but could eventually be expanded for broader purposes or in a wider range of circumstances, thereby raising the prospect of causing the harms related to this broadened use. One institution's use of FRT can also legitimize its use in other contexts and by other entities in the public or private sector, including where there are fewer safeguards implemented in order to prevent the deleterious impacts, misuse, and abuse of FRT.

For these reasons, impact assessments focused on privacy, automated decision-making or recommendation systems, and others with more holistic approaches would be important to undertake regarding FRT in the parliamentary context. Organizations, such as the Red Cross — that, in many ways, serve functions similar to government entities — have helpful policies on the treatment and handling of biometric data, which could be turned to and potentially implemented by government entities, in order to be in line with emerging best practices regarding such sensitive types of data.[223] Communication with the OPC, in particular, should be arranged if any privacy impact assessment is undertaken. Robust cybersecurity protocols should also be implemented and followed given the highly sensitive nature of biometric data and particularly facial images, which can be abused by adversaries and attackers for crimes such as identity fraud. Such assessments could also emphasize the importance of granting individuals the ability to access meaningful information about the logic involved in any automated decision using their facial image. Certain changes to Canada's legal regime regarding the treatment of facial images for automated processing, such as the requirement to obtain a warrant before such information is collected, could also mitigate proportionality issues related to FRT.

6.1.3 FRT and the Right to be Secure Against Unreasonable Search and Seizure

Constitutional Privacy and its Relationship with Other Human Rights

Canadians have the right to go about their daily lives without being subject to unreasonable state surveillance. This right is enshrined in section 8 of the *Canadian Charter of Rights and Freedoms*.[224] This section applies to both government laws and actions that interfere with the right to be free from unreasonable surveillance. Section 8 limits the surveillance activities of police officers and other law enforcement agencies, including border agents.[225]

Whether section 8 of the *Charter* can be used to limit the surveillance activities of the PPS will depend on whether parliamentary privilege applies to the use of face recognition within the parliamentary precinct and on Parliament Hill (in that particular use case). Regardless of whether the PPS is subject to the limitations that come with section 8 privacy rights, individuals who

visit Parliament Hill should be free to do so without being subject to unreasonable surveillance.

As discussed in **Section 3** of this report, Parliament is a symbol of Canada's democracy. It should welcome people from all backgrounds and political views. Part of this mission should be to guarantee a degree of anonymity regarding the activities that people undertake at the parliamentary precinct and Parliament Hill. This includes privacy and anonymity regarding the causes they visit Parliament to be informed about, to protest, or debate.[226] Interviews with experts highlighted that when individuals are subjected to unreasonable and disproportionate surveillance, they are likely to self-censor, leading to chilling effects on democratic speech and participation.[227] Instead, Parliament is a democratic institution where Canadians should feel confident that their privacy rights are respected.

When section 8 of the *Charter* does apply, the violation of privacy rights is established through a two-part analysis. First, courts consider whether there has been a 'search' or 'seizure' according to the legal principles that guide this analysis; and second, they consider whether the search is unreasonable.[228] Whether the individual has a reasonable expectation of privacy in relation to the subject matter of the search is the driving consideration in this analysis. This analysis is contextual and flexible, and relies on factors such as the place of the search; whether the individual has a direct or indirect interest in what is being searched; how invasive the technology is; and the nature of the information that is collected. It is clear in the case of face recognition searches that the individual has a direct and intimate interest in their face template information.

Regardless of whether the search through face recognition takes place while someone is in a public place, individuals' constitutional privacy rights are engaged. In the context of a use case that involves potentially identifying individuals throughout the parliamentary grounds and within Parliament buildings, the search conducted is not only of the face, but also of other information that can be ascertained about individuals from these observations. Face recognition technology and databases have the potential to aid the PPS in creating detailed and elaborate profiles of individuals based only on their face templates and visits to Parliament Hill.

Anonymity as an Essential Conception of Canadians' Constitutional Privacy Rights

As constitutional privacy principles develop to meet Canadians in the digital world, the right to anonymity has emerged as an essential aspect of our constitutional rights. Anonymity is not limited to activities that we undertake in private or in the comfort of our own homes. Anonymity is also not defined by attempts to hide one's identity. Instead, anonymity as a conception of privacy protects people in public, as well as in private, whether they are attempting to conceal their identity or not. As Justice Cromwell of the Supreme Court of Canada wrote in *R v Spencer*:[229]

> "The mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes him or her in public. Thus, in order to uphold the protection of privacy rights in some contexts, we must recognize anonymity as one conception of privacy."[230]

When an individual goes to Parliament Hill to attend a protest, their constitutional privacy rights should not disappear. Although they might be leaving the secrecy of their private life behind, the mere fact of attending a public protest should not mean that their privacy rights cease to exist.[231] The Supreme Court has recognized that individuals can have a reasonable expectation of privacy even in public places.[232] Mere presence in a public place does not give the PPS staff unfettered discretion to track individuals as they move across Parliament Hill.

Automated Surveillance Further Erodes Constitutional Privacy Rights

The right to privacy and anonymity in public is not absolute. Law enforcement and state agents are generally free to observe individuals in public places when they are not aided by surveillance technologies, such as cameras, records, or face recognition technology. However, when state agents employ the help of surveillance technologies to refine their observations, the reasonable expectation of privacy that individuals hold is heightened.[233] Several constitutional privacy cases decided by the Supreme Court of Canada have made it clear that privacy interests are heightened when state agents enhance their observations with more advanced technologies. For example, in *R v Wise*,[234] law enforcement tracked the location of an accused's vehicle on public highways through an electronic monitoring device.[235] The Supreme Court decided that, despite this information being "public" in nature (the movement of the car through highways), the use of a tracking device to monitor a person's movements without judicial authorization constituted an unreasonable search.[236] Similarly, when PPS staff observe Parliament Hill or the parliamentary precinct unaided by intrusive surveillance technologies, observing individuals as they move about, they may be engaging in legitimate surveillance activities. On the other hand, following a specific individual based on their facial template to identify them and/or track exactly where they are moving throughout the precinct, how long they visit for, and how often, could potentially amount to an unreasonable search. The tracking of face templates could be seen as tantamount to attaching an electronic monitoring device to the person, giving the PPS the opportunity to map out people's movements.

Privacy interests such as the ability to remain anonymous are heightened by the use of surveillance technologies, as well as their capacity to help state agents draw inferences about individuals.[237] In *R v Spencer*, the Supreme Court found that the warrantless acquisition of internet subscriber information violated Mr. Spencer's section 8 privacy rights.[238] According to the Supreme Court, Mr. Spencer had a reasonable expectation of privacy in his internet subscriber information, in part because of what it could be used to reveal, including his exact location, as well as his internet searches, visits, and activities. The Supreme Court's focus on inferences highlights that it is not only the information collected that matters, but also what it is used to reveal. In a potential use case where the PPS uses face recognition to recognize and collect information about individuals, the true subject matter of the search is not simply the person's face, but all the information that this collection and subsequent analysis can also be used to reveal.[239] First, and most importantly, facial information and templates can reveal someone's identity, particularly if matched with other data. When connected to the date that someone visits Parliament Hill, how often they do so, etc., it would also be possible to have enough information to build a profile of that individual.[240] This can reveal what kind of events people attend, what causes they might be in favour of, who

they meet with, and how often they engage in such activities.

Courts have already followed the lead of the Supreme Court on these important constitutional privacy issues. As a result, they have consistently found that the warrantless use of surveillance technologies to observe and reveal information about an individual in fact violates constitutional privacy protections. Courts in Ontario have identified privacy violations in the use of video surveillance systems that target public areas.[241] The use of advanced surveillance technologies, such as continuous video surveillance (especially when it is hidden or discreet), is accepted as posing a greater threat to individual privacy rights than the "discrete [sic] and purpose-oriented" collection of information.[242]

In conclusion, the potential use of FRT to identify visitors on parliamentary grounds and to match images against existing databases is more likely to engage constitutional privacy rights than the manual observance of visitors by PPS staff. There are numerous reasons why FRT systems may seem appealing to public safety actors. However, the increased surveillance that these systems enable would ultimately allow institutions to identify, track, and analyze faces and behaviour at a rate that no human could do on their own. As a result, more attention should be paid to the violations of privacy rights that would likely follow from the use of FRT in the parliamentary context, given the increasingly invasive nature of such systems.

Similar principles applied to the earlier sections on statutory privacy laws should be used here to moderate the impacts of FRT on the privacy rights of parliamentary visitors and the public that access both Parliament Hill and buildings within the parliamentary precinct. Any 'search' conducted by the PPS should be reasonable and carried out in a reasonable manner. The use of surveillance technologies should be limited in scope to minimize impairment only to the degree that it is necessary for their legitimate activities. This determination is contextual and requires a case-by-case analysis. The use of FRT to conduct mass surveillance of protest crowds on Parliament Hill, for example, is unlikely to meet this threshold. As such, the potential use of FRT and the protection of constitutional privacy rights should be conducted in line with the principles of minimal impairment, effectiveness, proportionality, and necessity discussed earlier.

6.1.4 Key Privacy Rights Considerations

- Face recognition technology and databases have the potential to aid PPS in creating detailed profiles of individuals based only on their face templates and visits to the parliamentary precinct and Parliament Hill.
- There are currently no binding laws that govern the collection and automated processing of facial information in Canada, such as through FRT.
- The privacy principles of necessity, proportionality, and their related considerations of effectiveness and minimal impairment, ought to inform the collection and processing of facial information through FRT in the parliamentary context.
- To justify the collection of highly sensitive biometric information, such as faces and the templates that can be made of a person's face, there must be a demonstrable need to collect and retain each piece of information. Any facial templates collected beyond a demonstrable need should be deleted immediately; and, if stored, should be de-

identified so as to be in accordance with the best practices regarding the storage of biometric information and to reduce the risk of privacy intrusions.

- The bulk capture of people's facial information without consent in the parliamentary context may amount to mass surveillance while challenging the right to the presumption of innocence.
- Certain decisions could be made that would aim to reduce the risks of FRT in terms of privacy rights and other rights protected by the *Charter*. Reducing how, when, where, and why FRT is used would be a first general set of steps that could be useful in mitigating the technology's risks. These limits include crafting specific, targeted purposes or triggers for its use; temporal limits on its use; limiting its use to the fewest geographic locations or to specific locations; and limiting whose facial images are scanned, compared, and stored.
- Impact assessments focused on privacy, automated decision-making or recommendation systems, and others with more holistic approaches would be important to undertake regarding potential use of FRT in the parliamentary context.

6.2 The Rights to Free Expression, Freedom of Assembly and Association

The right to free expression is one of the human rights most evidently pertinent to the activities of visitors to Parliament Hill. Individuals and groups from across Canada travel to the Hill to speak with parliamentarians, organize rallies and protests, and to make their voices heard on essential political issues. This section will explain how the use of FRT may impact the right to free expression in the parliamentary context. While FRT does not directly harm free expression, its use can give rise to chilling effects that are likely to dissuade many groups from organizing on important issues. Parliamentarians have already identified the impact of disproportionate security practices on free expression and public access.[243] The use of FRT is likely to reduce the opportunity for free expression and public access on the Hill, especially for those communities that have been historically subject to state surveillance and may fear further intrusion into their lives if they attend protests or events on Parliament Hill. It is therefore essential that the right to free expression and peaceful assembly is recognized and bolstered.

Canadians have the right to free expression and assembly under section 2 of the *Charter*.[244] The right to freedom of assembly is generally subsumed under freedom of expression in legal analysis. The *Charter* protects all expression regardless of its content.[245] A non-exhaustive list of protected expression includes protests, rallies, labour strikes, defamatory statements, pornography, and hate speech subject to certain limitations.[246] Like all rights in the *Charter*, freedom of expression is not absolute, and the government can limit the right if the limit is justifiable in a free and democratic society.[247] Ultimately, section 2 of the *Charter* is driven by three fundamental values that guide the courts' interpretation of freedom of expression as a right and its violations: self-fulfillment, democratic discourse, and truth finding.[248]

6.2.1 Location of Expression: Parliament as a Symbol of Democratic Ideals

The location where the expression takes place is significant to determining whether the rights to expression and assembly are at stake. The relationship between location

and expression rights is complicated. The historical character of the location in question may weigh in favour or against recognizing the protection of speech in such a place. On one hand, some locations with historic or public significance can raise expectations of constitutional protection for free expression because of what they represent.[249] On the other hand, the historical and actual function of a place may "suggest that expression within it would undermine the values underlying free expression."[250] If it is found to be the case that the place of expression is considered to be private (such as government worker offices), then this may weigh against recognizing expression as protected.

The state of these legal developments has unclear implications for the protection of free expression at Parliament Hill. Parliament Hill is a place of symbolic significance to Canadians and therefore invites the exercise of free expression. At the same time, for parliamentary functions to be carried out effectively, free expression and assembly activities are curtailed and regulated by the administration of both the Senate and the House of Commons.

Parliament buildings and its grounds hold great symbolic value for our country and democratic ideals. The exercise of free expression within the parliamentary precinct and Parliament Hill can be understood as the freedom to organize and participate in protests, rallies, and other gatherings on Parliament grounds.[251] The physical aspects of Canada's Parliament Hill are essential in the exercise of free expression on its grounds. The architecture of our parliamentary grounds is inviting to the public and has become a place of formal and informal gathering. These include protests, rallies, marches, vigils, and more casual leisure gatherings.[252] Canada's Parliament Hill is recognized as one of the most architecturally open (and accessible) national assemblies in the world,[253] alongside the German Bundestag located in Berlin and New Zealand's parliament located in Wellington.[254] Similar to the Canadian parliament, these two buildings are notable for offering open green space on their grounds that makes gatherings desirable and accessible.

Despite its public nature, there are regulations associated with using public grounds such as Parliament Hill.[255] Visitors who wish to use the outside grounds must first seek a permit.[256] They are required to communicate with the appropriate parliamentary staff to arrange the time and details of their gathering.[257] Where a group lacks a permit, they will be asked to leave the grounds. This practice has resulted in the norm of seeking permission for assemblies that take place on the Hill.

Ultimately, parliamentary grounds stand at a tension between maintaining order and security within the parliamentary precinct to allow for the efficient and safe exercise of parliamentary functions, and symbolizing the democratic ideals of openness and accessibility. While recognizing this tension, security practices should be enacted while minimizing their impact on the *Charter* rights of visitors to Parliament Hill. In the words of Professor Anne Dance, "[p]rotests might be managed and challenged… but they are still regarded as important to democracy… they are valued as an essential component of the Hill as a public space".[258]

6.2.2 The Chilling Effects of FRT

Security and surveillance practices have a direct impact on the ability of individuals to exercise their right to free speech. When an individual is, or suspects to be, a target of surveillance, they are less likely to exercise their right to free expression. This result is inconsistent with the democratic ideals that

define Parliament Hill and make it a forum for political expression. FRT has the potential to pose a threat to free expression. It is essential that any use or implementation of this technology considers the impact that each use case of this technology might have on the exercise of the constitutional right to free speech on parliamentary grounds. Freedom of expression at Parliament is likely to be 'chilled' by the use of face recognition technology, particularly if it is used in a broad or unregulated fashion — especially without judicial authorization and in a way that is opaque, shielding it from public scrutiny. Academic studies have established that state surveillance leads to chilling effects,[259] which can manifest as self-censorship or other forms of behaviour modification. Studies have predominantly focused on people's online behaviour. In a 2017 study, Jon Penney found that individuals experienced chilling effects following Edward Snowden's revelations about NSA surveillance.[260] Other studies have confirmed these findings; one study discovered shifts in people's online search behaviour (on Google) following the NSA event.[261] This body of research shows that when individuals are faced with a system of surveillance, they are more likely to self-censor or modify their behaviour to conform to socially accepted norms.[262] Interviews with experts reflected this concern about the relationship between surveillance and the chilling effects of FRT on freedom of expression in the parliamentary context. Experts highlighted that these chilling effects are likely to be more dramatic and pronounced when experienced by marginalized groups, such as racialized individuals, people with disabilities, religious minorities, and gender non-conforming individuals.

These academic findings have significant implications for the potential use of intrusive surveillance technologies such as FRT on parliamentary grounds and/or at building entrances. Such chilling effects could mean that individuals will be discouraged and fearful of participating in activities such as gatherings, vigils, or protests that they might otherwise support. In this way, the creation of chilling effects risks violating the *Charter* rights to free expression and assembly as it can have strong effects on its free exercise. Compared to FRT, there are security tactics available that are less intrusive and pose less risk to the right to free expression. Given the existence of these alternatives, it is difficult to see the necessity of FRT in light of the chilling effects it will have on the public who wish to visit and exercise their right to free expression on Parliament Hill.

Considering the chilling effects of FRT is significant for the potential deployment of the technology in exterior and interior contexts. Inside parliamentary buildings, the potential use of FRT to identify all those who walk the halls of the House and Senate may have chilling effects on both visitors and parliamentarians. In a hypothetical scenario where parliamentarians and their visitors are identified as they move through the buildings, these parties may feel less comfortable having certain meetings or associating with other individuals if they perceive that their whereabouts are consistently monitored and tracked. While this violation of freedom of association may be less evident than the cancellation of a protest, for example, it could constitute, subject to parliamentary privilege, a violation of the freedom of assembly and free speech. Outside of the buildings, on Parliament Hill, the chilling effects of FRT surveillance are perhaps more evident. As canvassed in **Section 6.1.3**, the use of FRT can harm privacy rights, in part because it allows for the advanced profiling of individuals' behaviours and likely eliminates any potential for anonymity. Anonymity, even in a public place like Parliament Hill, can serve for some individuals as an essential precursor to the

exercise of their free expression *Charter* rights. Individuals that may be subject to higher rates of misidentification by an FRT system, such as those who have experience with the criminal justice system, may wish to avoid frequenting a space where their presence will be subject to PPS scrutiny or logging. As a result, they may choose to forgo the option to exercise their free speech altogether. This is a damaging result in a democratic and diverse society like Canada.

Ultimately, the constitutional right to free expression exists, among other reasons, to encourage participation in social and political decision-making. The governance and policies for any FRT systems used by the PPS must pay attention to the unique character of the location and activities that the PPS protects. While the PPS is responsible for the physical security within the parliamentary precinct and on Parliament Hill, and for protecting the people who engage in the activities that take place within it, it does not carry out these functions in a vacuum. Where the use of FRT harms the constitutional right to free expression, the necessity, proportionality, rational connection to an objective, and minimal impairment of its use must be adequately addressed in order for any intrusion to be a reasonable and justifiable limit on someone's free expression rights. Different implementations of FRT will impact the right to expression and association to varying degrees, depending on where and how the technology is used. Careful attention should be paid to the parties that are impacted by these decisions, and how their political speech and activities may be chilled as a result of increased surveillance.

6.2.3 Key Considerations for Free Expression, Freedom of Assembly and Association

- Canadians enjoy the constitutional right to freedom of expression, assembly and association; and this right can only be curtailed within reasonable and justifiable limits.
- This constitutional right is essential to democratic governance and is inherently connected to the political process.
- Parliament Hill is symbolic of these ideals and there is an expectation of free expression on parliamentary grounds, despite the use of outside grounds being highly regulated to facilitate the security of parliamentary activities.
- The use of FRT systems may chill the exercise of free expression and freedom of association within parliamentary grounds. This result is antithetical to the Canadian and democratic values that Parliament Hill represents.

6.3 Equality Rights and the Right to Freedom from Discrimination

6.3.1 Equality Rights in Canada

Under section 15 of the *Charter of Rights and Freedoms*, all individuals are equal before and under the law.[263] This section protects individuals from discrimination on the basis of race, national or ethnic origin, colour, religion, sex, age or mental or physical disability, or any analogous grounds decided by the courts. Some recognized analogous grounds include sexual orientation, marital status, non-citizenship, and residence on or off a reserve.[264]

Section 15 of the *Charter* protects individuals from direct and indirect discrimination. The latter is also known as adverse impact

discrimination. Direct discrimination refers to law or actions that distinguish between individuals based on a protected characteristics (i.e., a ground identified in the *Charter* or an analogous ground). Indirect discrimination refers to instances where individuals are treated, or appear to be treated, in the same way, yet the outcome might be different. Discrimination lies in the different impact of a law or action on individuals where this impact further marginalizes and disadvantages people of a certain identity.[265] Canadian law adopts a substantive understanding of equality that focuses on the impacts of government action regardless of intent, not just the formal treatment of individuals.[266]

The Supreme Court held recently that discrimination occurs when a distinction "imposes burdens or denies a benefit in a manner that has the effect of reinforcing, perpetuating, or exacerbating disadvantage."[267] In the context of this report, this means that even if everyone is subject to face recognition technology on parliamentary grounds, what in fact matters is whether in effect someone faces a higher burden (subject to increased surveillance when visiting parliament) or is denied a benefit that might be otherwise available to others. For example, if an individual is denied entry to Parliament Hill because the technology is more likely to consider that person a risk or if it misidentifies them because they are racialized or gender non-conforming, for example, they are not benefitting from the ability to enter Parliament, speak with their MP, or watch proceedings without this burden in the same the way that a white or cisgender person in that use case would. While there is no positive or absolute right to enter the parliamentary precinct or to watch proceedings, this technology could dissuade people from visiting parliamentarians, communicating with parliamentary offices, and watching debates and proceedings that they are interested in. This could potentially be conceptualized as the denial of a benefit. Individuals could also be approached by, and required to interact with, PPS officers more than others due to the discriminatory impacts of FRT systems. This can be conceptualized as the imposition of a burden on some individuals and not others. In some cases, these interactions could become detentions that lead to external police involvement, further worsening the situation faced by those who are brought to the attention of the PPS by the FRT system.

6.3.2 Bias in Face Recognition Algorithms and Equality Rights

Several academic studies and industry-wide assessments of AI-based technologies have gathered strong evidence of algorithmic bias and error rates. These studies indicate that face recognition technologies exhibit higher error rates when identifying racialized individuals and women in particular. A recent study by the NIST found that the adoption of AI technologies "come with significant downsides to individuals and society through the amplification of existing biases".[268] More specifically, the study found that "accuracy of FRT gender identification can vary with respect to the age and ethnic group" and that "biases can occur due to a lack of awareness about the multiplicity of gender".[269] As discussed in **Section 4.1.1**, AI experts Buolamwini and Gebru found that, among the various demographics they examined, FRT was more likely to misidentify "darker-skinned females", with error rates of up to 34.7%.[270] The studies mentioned in **Section 4.1.1** highlight FRT's higher rates of inaccuracy particularly for Black people, East Asian people, women, elderly people, and gender-non-conforming people. These aspects of identity may also intersect with each other, further compounding the possibility and harms of discrimination.[271] Taken all together, these findings point

to inaccuracies in FRT that stem from technological and human (social) sources. These inaccuracies impact gender and racial minorities more than other groups in particular. Where these technologies are used and have a negative impact on a specific group, the public institution that uses them would likely be in violation of the *Charter*'s equality guarantees.

Given the recent emergence of face recognition technologies, it is worth considering the discriminatory impacts that arise from the use of AI-based technologies generally. For example, a recidivism tool used by United States courts and probations officers, known as COMPAS, was found to discriminate against Black defendants. A study of the tool found that "[B]lack defendants were far more likely than white defendants to be incorrectly judged to be at a higher risk of recidivism, while white defendants were more likely than [B]lack defendants to be incorrectly flagged as low risk".[272] In the employment sector, there is a growing body of scholarly work that raises concerns about the implications of using AI software to recruit and select candidates, particularly in light of the way these technologies impact candidates who are women.[273]

Concerns about error rates and algorithmic bias are not purely hypothetical. Bias in face recognition technologies has already negatively impacted the lives of people in drastic and irreversible ways.[274] In the U.S., three cases of Black men who were misidentified by face recognition technology and subsequently arrested made national headlines.[275] These stories highlight the discriminatory outcomes that can result from the existence of such bias and error rates in AI, or even the *risk* of such errors. Where FRT that has unequal error rates among different groups is used in a location, those who are more likely to be misidentified due to their race, age, gender or other characteristics will also experience a higher risk of being wrongly arrested, misidentified, held in detention, and a host of other disadvantages under the law. It is therefore imperative that the impacts of these technologies on equity-deserving communities be considered and addressed before and during the deployment of such technology.

Issues of algorithmic bias have not yet been directly addressed by Canadian courts. This is not because these issues and rights violations do not exist, but rather because corporate secrecy, combined with limited legal pathways, make it difficult for individuals to bring claims forward. Despite the lack of concrete pronouncement on the issue, some cases are instructive of the harms and legal consequences of racial profiling and the use of biased technologies. In *Ewert v Canada*,[276] the Supreme Court of Canada reviewed the use of psychological and risk assessment tools by Correctional Services Canada for Indigenous inmates. The case is instructive for its finding that, in order to meet its obligation that information used by CSC was "as accurate and complete as possible", the state actor had to ensure that the results generated by the tools were valid when applied to Indigenous offenders.[277] Experts have also identified the Supreme Court case *R v Le* as instructive in how an individual's experience with race can be an "aggravating factor" in determining whether that person is detained by police.[278] For our purposes, the case points to the duty that courts now have to consider how an individual's experience with police detention may be different depending on their experience with race and historic facts about race relations. In the UK, the use of live face recognition by the South Wales police, as mentioned earlier in this report, was found to be discriminatory by the Court of Appeal. In *R (Bridges) v Chief Constable of South Wales*, the court ruled that the

police force that adopted FRT did not meet its obligation to do all that it reasonably could to address whether bias emerged from the use of live FRT.[279] Police, according to the law that governs them and the court's interpretation, had a positive duty to consider the bias issues posed by the FRT systems they used before implementation. The court accepted expert evidence that FRT systems are likely to be biased and have error rates, and concluded that this was evident enough to require pre-emptive measures prior to the use of FRT on individuals.

The issue of technological bias, understood as error rates in identifying diverse faces, is one of the ways in which FRT can be discriminatory. This section has surveyed the current state of studies on bias regarding FRT. Given the academic consensus on misidentification and bias rates for face recognition systems, it would be ill-advised to implement FRT without conducting proper assessments and understanding the risks it poses comparatively to different groups of people. Given these findings, the deployment of FRT, even if no action is taken based on its use, is likely to violate the equality section 15 rights of individuals who visit and access parliamentary grounds.[280]

6.3.3 Using FRT Risks Perpetuating Historical Disadvantages of Marginalized Communities

Discriminatory risks from the use of FRT emanate not only from technical inaccuracies with these systems, but also from the social context within which they are used. **Section 5.3.2** canvassed some of the issues that parliamentarians from racialized backgrounds have faced while serving their constituencies. Face recognition systems will not remove these biases, and in fact are likely to worsen and further entrench them. Where FRT algorithms are more likely to misidentify parliamentarians from racial, ethnic, and gender minorities, the PPS's reliance on these results without appropriate safeguards will increase feelings of unease and a lack of safety among these parliamentarians.

The same logic extends to people who are visitors to Parliament Hill. Historic disadvantages of marginalized groups will be exacerbated by the use of FRT surveillance on two fronts: first, because FRT systems rely on databases that are built on long-term societal biases, such as racism in the criminal justice system; and second, because interactions between security and law enforcement agencies with marginalized groups can lead to further insecurity and even criminalization for these groups.

When using face recognition technology, the PPS would have to rely on photo (or face template) databases. In security contexts, one common sense use of FRT is to identify potential threats. In the parliamentary context, one can imagine the use of FRT to identify visitors on Parliament Hill against images of known or potential threats; databases of individuals involved in the criminal justice systems (such as mugshot databases); or other databases that may be held and shared among law enforcement or other intelligence agencies. Once again here, the data-sharing practices discussed in **Section 5.2** are a key consideration. Who constitutes a 'threat' on parliamentary grounds must be carefully considered so as not to be overinclusive. As an example, careful consideration would be warranted to eliminate profiles of individuals not charged or had their charges dropped or expunged. It is well-accepted that racialized groups are more likely to be arrested and criminalized by our legal system. The identification of threats on Parliament Hill through FRT risks perpetuating these cycles of criminalization.

In addition to the design of the FRT system and the information it uses to reach its outputs, the manner in which the outputs are operationalized by the PPS may lead to discriminatory outcomes. As mentioned earlier in this report, it is essential that any interaction with a visitor that is initiated or caused by an FRT system's recommendation be verified and vetted by humans. While this will not eliminate the risk of bias or the discriminatory impact of the technology, it may reduce the risk of worsening the experience of someone who is otherwise free to move around the Hill unimpeded. Second, it is essential that the decisions of PPS personnel to approach or track individuals based on FRT matches be made on a reasonable and justifiable basis, and not simply because someone matches with a database that has little to no bearing with Parliament's physical security. Since the technology is more likely to give false positives on racialized individuals, for example, then taking actions such as detaining someone for arrest by law enforcement can have significantly increased detrimental impacts on the rights and liberties of these individuals than others.

6.3.4 Key Equality Rights Considerations

- Section 15 of the *Charter* guarantees that individuals are equal before and under the law; and guarantees that the individuals are protected from direct and indirect discrimination.
- An action or law is discriminatory when it imposes a burden or denies a benefit to a group of people. Courts pay attention to how the law perpetuates disadvantages historically faced by some groups.
- FRT has higher inaccuracy rates for racialized individuals and others belonging to historically marginalized groups. If a security entity acts on such outputs, the action is likely to be a violation of the individual's section 15 equality rights.
- Even if FRT becomes perfectly accurate, discrimination may arise from the databases that the PPS could use to feed the FRT system, and how its personnel act upon its findings.
- Using large databases from other law enforcement and intelligence agencies for an FRT system's watchlists risks further criminalizing groups of people who are disproportionately represented in such databases, because of the historic over-policing of these communities.

Appendix A: Clarifications from the Parliamentary Protective Service

The following clarifications have been provided by the PPS:

- The PPS would like to clarify that it "does not have access, nor is pursuing access to data banks used for FRT purposes."
- The PPS would like to specify that it engages in monitoring and not surveillance. For the PPS, "monitoring is a general term that refers to the systematic, continual, and active or passive observation of persons, places, things, or processes. By contrast surveillance is used to indicate targeted monitoring of activities by police or security officials for specific evidence of crimes or other wrongdoing."
- Regarding the right to free expression, freedom of assembly, and association considerations in the parliamentary context, the PPS would like to clarify that "our Parliamentarians greatly value access to Hill as well as the rights outlined herein. The PPS ultimately acts in accordance to our parliamentary stakeholders and supports these rights and is extremely sensitive to the rights described and acts to protect these rights every day."

Appendix B: Parliament of Canada Act (Excerpt)

Parliament of Canada Act
R.S.C., 1985, c. P-1

Parliamentary Protective Service

Interpretation

Definitions

79.51 The following definitions apply in this section and in sections 79.52 to 79.59.

Parliamentary Precinct means the premises or any part of the premises, other than the constituency offices of members of Parliament, that are used by the following entities or individuals or their officers or staff, and that are designated in writing by the Speaker of the Senate or the Speaker of the House of Commons:

a. the Senate, House of Commons, Library of Parliament or Parliamentary committees;

b. members of the Senate or the House of Commons who are carrying out their parliamentary functions;

c. the Senate Ethics Officer or the Conflict of Interest and Ethics Commissioner;

d. the Service; or

e. the Parliamentary Budget Officer. (*Cité parlementaire*)

Parliament Hill means the grounds in the City of Ottawa bounded by Wellington Street, the Rideau Canal, the Ottawa River and Kent Street. (*Colline parlementaire*)

Service means the office to be called the Parliamentary Protective Service that is established by subsection 79.52(1). (*Service*)

Establishment and Mandate

Establishment

79.52 (1) There is established an office to be called the Parliamentary Protective Service.

Speakers responsible

(2) The Speaker of the Senate and the Speaker of the House of Commons are, as the custodians of the powers, privileges, rights and immunities of their respective Houses and of the members of those Houses, responsible for the Service.

Mandate

79.53 (1) The Service is responsible for all matters with respect to physical security throughout the parliamentary precinct and Parliament Hill.

Capacity

(2) In carrying out its mandate, the Service has the capacity of a natural person and the rights, powers and privileges of a natural person.

Financial and administrative matters

(3) Despite sections 19.3 and 52.3, the Service shall act on all financial and administrative matters with respect to the Service and its staff.

Director of Service

Director

79.54 (1) There shall be a Director of the Parliamentary Protective Service who is to be selected in accordance with the terms of the arrangement entered into under section 79.55.

Integrated security operations

(2) The Director shall lead the integrated security operations throughout the parliamentary precinct and Parliament Hill under the joint general policy direction of the Speaker of the Senate and the Speaker of the House of Commons.

Control and management of Service

(3) The Director has the control and management of the Service.

Arrangement for Physical Security Services

Arrangement

79.55 (1) The Speaker of the Senate and the Speaker of the House of Commons, being responsible for the Service, and the Minister of Public Safety and Emergency Preparedness shall enter into an arrangement to have the Royal Canadian Mounted Police provide physical security services throughout the parliamentary precinct and Parliament Hill.

RCMP to provide services

(2) The Royal Canadian Mounted Police shall provide the physical security services in accordance with the terms of the arrangement.

Selection process for Director

79.56 (1) The arrangement entered into under section 79.55 shall provide for a process for selecting a person to act as the Director of the Parliamentary Protective Service. It shall also provide for a person — identified by name or position — to act as the Director on an interim basis if the Director is absent or incapacitated or if the office of Director is vacant, and set out the maximum period that the person may act as the Director on an interim basis.

Member of RCMP

(2) The Director, or the person acting as the Director on an interim basis, must be a member as that term is defined in subsection 2(1) of the Royal Canadian Mounted Police Act.

Estimates

Estimates to be prepared and transmitted

79.57 Before each fiscal year, the Speaker of the Senate and the Speaker of the House of Commons shall cause to be prepared an estimate of the sums that will be required to pay the expenditures of the Service during the fiscal year and shall transmit the estimate to the President of the Treasury Board, who shall lay it before the House of Commons with the estimates of the government for the fiscal year.

Powers, Privileges, Rights and Immunities

For greater certainty

79.58 For greater certainty, nothing in sections 79.51 to 79.57 shall be construed as limiting in any way the powers, privileges, rights and immunities of the Senate and the House of Commons and their members.

General

Statutory Instruments Act

79.59 For greater certainty, the designation referred to in the definition parliamentary precinct in section 79.51 is not a statutory instrument for the purposes of the *Statutory Instruments Act*.

Appendix C: Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

Between

THE SPEAKER OF THE SENATE,

THE SPEAKER OF THE HOUSE OF COMMONS,

THE MINISTER OF PUBLIC SAFETY AND EMERGENCY PREPARDNESS, and

THE COMMISSIONER OF THE RCMP

WHEREAS, the House of Commons resolved:

> That this House, following the terrorist attack of October 22, 2014, recognize the necessity of fully integrated security throughout the Parliamentary precinct and the grounds of Parliament Hill, as recommended by the Auditor General in his 2012 report and as exists in other peer legislatures; and call on the Speaker, in coordination with his counterpart in the Senate, to invite, without delay, the Royal Canadian Mounted Police to lead operational security throughout the Parliamentary precinct and the grounds of Parliament Hill, while respecting the privileges, immunities and powers of the respective Houses, and ensuring the continued employment of our existing and respected Parliamentary Security staff;

AND WHEREAS, the Senate resolved:

> That the Senate, following the terrorist attack of October 22, 2014, recognize the necessity of fully integrated security throughout the Parliamentary precinct and the grounds of Parliament Hill, as recommended by the Auditor General in his 2012 report and as exists in other peer legislatures; and call on the Speaker, in coordination with his counterpart in the House of Commons, to invite, without delay, the Royal Canadian Mounted Police to lead operational security throughout the Parliamentary precinct and the grounds of Parliament Hill, while respecting the privileges, immunities and powers of the respective Houses, and ensuring the continued employment of our existing and respected Parliamentary Security staff;

The Speaker of the Senate and the Speaker of the House of Commons, in the exercise of the privileges of their respective Houses, hereby invite the RCMP to lead operational security throughout the Parliamentary precinct and the grounds of Parliament Hill;

THE OBJECTIVE OF THIS MEMORANDUM OF UNDERSTANDING IS TO SET OUT THE FOLLOWING PRINCIPLES FOR THE CREATION OF A PARLIAMENTARY PROTECTIVE SERVICE:

Parliamentary Protective Service

1. The Parties agree that there shall be established the Parliamentary Protective Service. The Speaker of the Senate and the Speaker of the House of Commons are, as the custodians of the powers, privileges, rights and immunities of their respective Houses and of the members of those Houses, responsible for the Service.

2. The Parliamentary Protective Service is established to provide integrated physical security throughout the Parliamentary precinct and the grounds of Parliament Hill, in accordance with this MOU.

3. Physical security is all the measures taken that are necessary to provide for the physical protection of the grounds of Parliament Hill and the Parliamentary Precinct, including the security of Parliament, its premises, Parliamentarians, Parliamentary Staff, and guests of Parliament, as well as all visitors to the grounds and/or the Precinct, and any assets located within or events that take place therein. For greater certainty, the Parties agree that this definition excludes IM/IT infrastructure and IT security, including the sharing and protection of data.

   This definition will be further clarified by the transition team which will also identify roles and responsibilities.

4. The Parliamentary Protective Service will include members of the RCMP, and of the current House of Commons and Senate Protective Services.

Selection and Appointment of Director

5. The Director of the Parliamentary Protective Service shall be an RCMP member appointed by the Commissioner. Before appointing the Director, the Commissioner will consult with the Speaker of the Senate and the Speaker of the House of Commons and they shall participate in the selection process for such appointment. The process shall be consensus based.

6. In the event that the Director is absent or unable to act or the office is vacant, the next most senior and highest ranking RCMP member within the Parliamentary Protective Service will serve as Director. The interim Director shall not act in the position for a period exceeding 180 days.

Governance

7. The Parties recognize that:

    a. the authority for security of the Parliamentary precinct is vested in the Speaker of the Senate and the Speaker of the House of Commons, as the custodians of the privileges, rights, immunities and powers on behalf of their respective Houses and of the members of those Houses, as per the Constitution of Canada and the *Parliament of Canada Act*;

    b. The RCMP will lead integrated security operations throughout the Parliamentary precinct and on the grounds of Parliament Hill. The Commissioner of the RCMP, under the direction of the Minister of Public Safety and Emergency Preparedness, and in accordance with the principle of policing independence, has the control and management of the RCMP and all matters connected therewith.

8. The Speaker of the Senate and the Speaker of the House of Commons will set general policy, including annual objectives, priorities and goals related to the security of the Parliamentary precinct and Parliament Hill, in consultation with the Director. As part of the consultation, the Director will:

    a. provide information pertaining to the security of the Parliamentary precinct, Parliament Hill and the operational and administrative status of the Parliamentary Protective Service; and

    b. provide information relating to the deployment of Parliamentary Protective Service personnel and materiel.

9. The Speakers will advise the Director of those buildings or places that comprise the Parliamentary precinct and will consult the Director with regards to any changes to the premises to be included in the Parliamentary precinct.

Operations

10. The Director will be responsible for planning, directing, managing and controlling operational parliamentary security, including members of the RCMP, House of Commons and Senate Protective Services, taking into account the objectives, priorities and goals as set by the Speaker of the Senate and the Speaker of the House of Commons.

11. In its mandate and organization, and through the duties and activities of its members, the integrated Parliamentary Protective Service shall:

    a. be sensitive and responsive to, and act in accordance with, the privileges, rights, immunities and powers of the Senate and the House of Commons and their Members;

b. provide physical security in the Parliamentary precinct and on the grounds of Parliament Hill including the physical security of Parliament, its premises, Parliamentarians, Parliamentary Staff, and guests of Parliament. Allegations and complaints of criminal activity will be referred to appropriate police officers outside the Parliamentary Protective Service and subsequent policing activities will follow established protocols consistent with parliamentary privileges and traditions;

c. allow such other branches of the RCMP, such as the Prime Minister's Protective Detail, to carry out their functions within the Parliamentary precinct in accordance with such protocols that may be established with such branches; and

d. have due regard to the need to ensure reasonable access to the Parliamentary precinct and the grounds of Parliament Hill.

12. The Speakers shall, in consultation with the RCMP, establish a protocol with respect to operational security for parliamentary proceedings, and any other protocol as may be required.

Funding, Budget and Estimates

13. For operational efficiency and proper accountability, the Parliamentary Protective Service will be funded through a single vote under Parliament.

14. Upon the establishment of the Parliamentary Protective Service, the funding that was appropriated by Parliament to defray the operational expenditures of

    a. the RCMP,
    b. the Senate in relation to the Senate Protective Service, and
    c. the House of Commons in relation to the House of Commons Protective Service

    related to the Parliamentary precinct and the grounds of Parliament Hill, and that is unexpended on the date the Service is established, will continue to be used by these entities to pay for the respective entities' operational costs until such time as the Parliamentary Protective Service is able to receive a transfer through an appropriation to the Service. If needed, the Director will seek additional funding in the year of the implementation through the Estimates process.

15. Prior to each fiscal year, the Director, will consult any individuals or entities, including the RCMP, the House of Commons, the Senate, the Library of Parliament, to ascertain security requirements, including planned or anticipated events, for the Parliamentary precinct and the grounds of Parliament Hill and will prepare a draft estimate, for the approval of both Speakers, of the sums that will be required to pay the charges and expenses relating to the Parliamentary Protective Service during the fiscal year.

16. The Speakers will jointly consider the draft estimate, establish an estimate and, upon their approval, transmit it to the President of the Treasury Board, who shall lay it before the House of Commons with the estimates of the government for the fiscal year.

17. The Parliamentary Protective Service, through its Director, may enter into agreements with the Senate, House of Commons, or the RCMP for the provision of administrative services to support the Parliamentary Protective Service.

18. The expenses incurred by the RCMP, the House of Commons and the Senate, upon establishment of the Parliamentary Protective Service and in accordance with this Memorandum of Understanding, will be reimbursed by the Parliamentary Protective Service through an Interdepartmental Settlement.

Implementation

19. The Parties shall work together:

> (*a*) to determine the most suitable means of implementing the objectives described in this Memorandum of Understanding; and
> (*b*) to draft any further Memoranda of Understanding the Parties consider necessary to implement the objectives described in this Memorandum of Understanding;

20. A transition team, with representation chosen by the Parties, will be established upon signing of this Memorandum of Understanding, and will address all necessary issues including, but not limited to, clarifying the roles and responsibilities of the RCMP and the Parliamentary Protective Service, organizational restructuring, recruitment, training and development and labour relations.

21. The Parties recognize and accept the requirement to transition existing personnel employed by the House of Commons and Senate Protective Services to appropriate functions in the Parliamentary Protective Service, based on a commitment of continuous employment.

22. The Parties will make best efforts to develop and implement a joint Communications Plan in regard to the Parliamentary Protective Service. Until such a plan is in place, the Parties will make reasonable efforts to consult each other with respect to any public communications in regard to the Parliamentary Protective Service.

Dispute Resolution

23. In the event of a dispute arising from the interpretation or operation of this Memorandum of Understanding, it will be referred to the Parties, or their representative designates, who will use their best efforts to resolve the matter amicably.

Review

24. The Parties, or their representative designates, will co-operate and communicate openly with each other on any matter relating to the administration of this Memorandum of Understanding and will meet as required and/or at least annually to review the operation and effectiveness of this Memorandum of Understanding.

Amendments to the Memorandum of Understanding

25. This Memorandum of Understanding may only be amended by the written consent of the Parties.

Termination

26. Any Party to this Memorandum of Understanding may terminate it at any time, upon one year written notice to the other Parties.

Effective Date and Signature

27. This Memorandum of Understanding will become effective upon the date of the last signature and will remain in effect until such time as one of the Parties gives notice for termination.

IN WITNESS WHEREOF the Parties hereto have agreed to this Memorandum of Understanding through duly authorized representatives.

References

[1] David O Manz & Thomas W Edgar, *Research Methods for Cyber Security*, (Cambridge, MA: Elsevier, 2017) at 95–130.

[2] Esha Patnaik, "Reflexivity: Situating the Researcher in Qualitative Research" (2013) 2:2 *Humanities and Social Science Studies* 98, online: www.researchgate.net/publication/263916084_Reflexivity_Situating_the_researcher_in_qualitative_research.

[3] House of Commons, *October 22, 2014: House of Commons Incident Response Summary* (3 June 2015) at 1 [House of Commons, *Incident Response Summary*].

[4] Mark Bourrie, *Canada's Parliament Buildings* (Toronto: Dundurn Press, 1996) at 11.

[5] *Weisfeld v Canada*, [1995] 1 FC 68, 1994 CanLII 3503 (FCA) [*Weisfeld v Canada*].

[6] "Parliament Hill tourist facilities overwhelmed", *CTV News* (6 May 2007), online: www.ctvnews.ca/parliament-hill-tourist-facilities-overwhelmed-1.240173.

[7] *R v Strebakowski*, [1995] BCJ No 1722, 1995 CanLII 1845 (BC SC).

[8] *Order PO-1747 Appeal PA-980336-1*, 2000 CanLII 20933 (ON IPC), online: https://www.canlii.org/en/on/onipc/doc/2000/2000canlii20933/2000canlii20933.pdf.

[9] *Rowe v Unum Life Insurance Company of America*, [2006] OJ No 1897, 2006 CanLII 15772 (ON SC).

[10] "Indigenous Peoples Space: Building the Future Together", online: *Assembly of First Nations* www.afn.ca/indigenous-peoples-space-building-the-future-together/; Ian Austen, "Vast Indigenous Land Claims in Canada Encompass Parliament Hill", *The New York Times* (12 November 2017), online: www.nytimes.com/2017/11/12/world/canada/canada-first-nations-algonquin-land-claims.html.

[11] See e.g., Senate Canada, *How Did We Get Here? A Concise, Unvarnished Account of the History of the Relationship Between Indigenous Peoples and Canada: Interim Report Standing Senate Committee on Aboriginal Peoples* (April 2019) (Chair: Lillian Dyck).

[12] *Ibid* at 3.

[13] *Honouring the Truth, Reconciling for the Future: Summary of the Final Report of the Truth and Reconciliation Commission of Canada* (Ottawa: Truth and Reconciliation Commission of Canada, 2015) at 1 and 266; Andrew Crosby and Jeffrey Monaghan, *Policing Indigenous Movements: Dissent and the Security State* (Black Point & Winnipeg: Fernwood Publishing, 2018).

[14] Courtney Dickson and Bridgette Watson, "Remains of 215 children found buried at former B.C. residential school, First Nation says", *CBC News* (29 May 2021), online: www.cbc.ca/news/canada/british-columbia/tk-eml%C3%BAps-te-secw%C3%A9pemc-215-children-former-kamloops-indian-residential-school-1.6043778; "Canada: 751 unmarked graves found at residential school", *BBC* (24 June 2021), online: www.bbc.com/news/world-us-canada-57592243. At the time of writing, unmarked graves continue to be searched for and are being identified by Indigenous communities.

[15] "Mandate Letters" (16 December 2021), online, *Prime Minister of Canada, Justin Trudeau*: pm.gc.ca/en/mandate-letters.

[16] *Truth and Reconciliation Commission of Canada: Calls to Action*, (Winnipeg: Truth and Reconciliation Commission of Canada, 2015) ss. 30, 383; Kanika Samuels-Wortley, "To Serve and Protect Whom? Using Composite Counter-Storytelling to Explore Black and Indigenous Youth Experiences and Perceptions of the Police in Canada" (2021) 67:8 *Sage Journals*, online: doi.org/10.1177/0011128721989077.

[17] Some changes to aspects of our faces may be possible in certain circumstances, such as the existence of medical ailments, physical disabilities, or elective surgeries.

[18] The terms 'information' and 'data' are used interchangeably throughout this report.

[19] As briefly examined in **Section 4.2,** there has been a significant push to collect and measure such biometric information, particularly following the events of 9/11, with a view to sort people based on their perceived level of risk to society. See e.g., Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Durham, NC: Duke University Press, 2011); Benjamin J Muller, "Global Surveillance and Policing: Borders, Security, Identity" in Elia Zureik & Mark B Salter, eds, *Global Surveillance and Policing: Borders, Security, Identity* (Portland: Willan Publishing, 2005) 83.

[20] The anthropomorphization of technology can obfuscate the fact that humans have programmed and developed such technology, and can lead to emotional attachment to technology's processes and results. See e.g., Erick Hermann "Anthropomorphized Artificial Intelligence, Attachment, and Consumer Behaviour" (2022) 33 *Marketing Letters* 157, online: doi.org/10.1007/s11002-021-09587-3.

[21] Christiane Wendehorst & Yannic Duller, "Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces" (August 2021) at 12–13, online (pdf): *Policy Department for Citizen's Rights and Constitutional Affairs, European Parliament* www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf [Wendehorst & Duller, *Biometric Recognition*].

[22] Tamir Israel, "Facial Recognition at a Crossroads: Transformation at our Borders and Beyond" (30 September 2020) at 12–14, online (pdf): *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)* cippic.ca/uploads/FR_Transforming_Borders.pdf [Israel, *Facial Recognition at a Crossroads*].

[23] Insaf Adjab et al, "Past, Present, and Future of Face Recognition: A Review" (2020) 9:8 *Electronics* at 15–31, online: www.mdpi.com/2079-9292/9/8/1188/htm [Adjab et al, *Past, Present, and Future*].

[24] Pete Fussey & Daragh Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology" (July 2019), online (pdf): *Human Rights Centre: University of Essex* repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf [Fussey & Murray, *Independent Report*]; Pete Fussey & Daragh Murray, "Policing Uses of Live Facial Recognition in the United Kingdom" (2020), online (pdf) *AI Now Institute* https://ainowinstitute.org/regulatingbiometrics-fussey-murray.pdf.

[25] "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta" (2 February 2021), online: *Office of the Privacy Commissioner of Canada* www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/ [Privacy Commissioner, *Joint investigation*].

[26] Wendehorst & Duller, *Biometric Recognition* at 20; Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun & Kate Gilbert, "Facial Recognition Briefing #1" (August 2020), *TIP – Tech Informed Policy*, online: http://techinformedpolicy.ca/facial-recognition-briefing-1/; Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun & Kate Gilbert, "Facial Recognition Briefing #2" (August 2020), *TIP – Tech Informed Policy*, online: http://techinformedpolicy.ca/facial-recognition-briefing-2/.

[27] Wendehorst & Duller, *Biometric Recognition* at 20; Luke Stark & Jevan Hutson, "Physiognomic Artificial Intelligence" (last revised 14 February 2022) [forthcoming in *Fordham Intellectual Property, Media & Entertainment Law Journal*], online (pdf): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927300.

[28] Anil Jain, "Expert Report of Dr Anil Jain" (30 September 2018) at para 19, online (pdf): *High Court of Justice: Queen's Bench Division – Administrative Court* www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/First-Expert-Report-from-Dr-Anil-Jain.pdf [Jain, *Expert Report*].

[29] Bethan Davies, Martin Innes & Andrew Dawson, "An Evaluation of South Wales Police's Use of Automated Facial Recognition" (September 2018) at 11, online (pdf): *Universities' Police Science Institute: Crime & Security Research Institute (Cardiff University)* static1.squarespace.com/static/51b06364e4b02de2f57fd72e/t/5bfd4fbc21c67c2cdd692fa8/1543327693640/AFR+Report+%5BDigital%5D.pdf [Davies, Innes & Dawson, *An Evaluation*]; Fussey & Murray, *Independent Report* at 10-11.

[30] *R (Bridges) v Chief Constable of South Wales Police & Information Commissioner*, [2020] EWCA Civ 1058 [*Bridges v CCSW Police & Information Commissioner*].

[31] Enjie Jiang, "A review of the comparative studies on traditional and intelligent face recognition methods" (2020) *2020 International Conference on Computer Vision, Image and Deep Learning* 11, online: https://ieeexplore.ieee.org/abstract/document/9270454 [Jiang, *Traditional and intelligent face recognition methods*].

[32] Davies, Innes & Dawson, *An Evaluation*.

[33] The security assessment of closed-source or proprietary software can also be outsourced to third parties. See e.g., Yuan Stevens et al, "See Something, Say Something: Coordinating the Disclosure of Security Vulnerabilities in Canada" (June 2021), online: *Cybersecure Policy Exchange* https://www.cybersecurepolicy.ca/vulnerability-disclosure.

[34] There are numerous legal issues raised by developments in the field of AI, see e.g., Florian Martin-Bariteau & Teresa Scassa, "Introduction" in Florian Martin-Bariteau & Teresa Scassa, eds, *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021) 1; Filippo A Raso et al, "Artificial Intelligence & Human Rights: Opportunities & Risks" (25 September 2018) *Berkman Klein Centre Research Publication No 2018-6,* online: papers.ssrn.com/sol3/papers.cfm?abstract_id=3259344; Mark Latonero, "Governing Artificial Intelligence: Upholding Human Rights & Dignity" (10 October 2018), online (pdf): *Data & Society Research Institute* datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf.

[35] Adjab et al*, Past, Present, and Future* at 22.

[36] *Ibid*.

[37] A significant amount of human labour is needed for the creation of AI systems, including the labelling and categorizing of training datasets. See e.g., Mary L Gray & Siddharth Suri*, Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*, (Boston: Houghton Mifflin Harcourt, 2019).

[38] See e.g., Adjab et al*, Past, Present, and Future* at 6–14.

[39] Richard Van Noorden, "The ethical questions that haunt facial-recognition research", *Nature* (18 November 2020), online: www.nature.com/articles/d41586-020-03187-3.

[40] Peter Dayan, "Unsupervised Learning", in Robert Wilson and Frank Keil, eds, *The MIT Encyclopedia of the Cognitive Sciences* (Cambridge, MA: MIT Press, 1999), online: *Princeton* web.math.princeton.edu/~sswang/developmental-diaschisis-references/dun99b.pdf.

[41] Frank Pasquale*, The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

[42] *Canadian Charter of Rights and Freedoms*, ss. 7, 9, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11 [*The Charter*]. See also: Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (1 September 2020) at 123–134, online: *Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) and the International Human Rights Program (Faculty of Law, University of Toronto)* citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/ [Robertson, Khoo & Song, *To Surveil and Predict*].

[43] See e.g., Jain, *Expert Report* at 7–10; Adjab et al*, Past, Present, and Future*; Davies, Innes & Dawson, *An Evaluation*; Fussey & Murray, *Independent Report*; Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data" (16 May 2019), online*: Georgetown Law: Centre on Privacy & Technology* www.flawedfacedata.com/ [Garvie, *Garbage In, Garbage Out*].

[44] Jiang, *Traditional and intelligent face recognition methods.*

[45] danah boyd, "Undoing the Neutrality of Big Data" (2016) 67 *Fla L Rev* 226; Leah West, "Ethical Applications of Big Data-Driven AI on Social Systems: Literature Analysis and Example Deployment Use Case" (2020) 11: 235 *Information* 2020, online: https://ssrn.com/abstract=3659253.

[46] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (*Proceedings of Machine Learning Research delivered at the Conference on Fairness, Accountability, and Transparency*, February 2018), online: https://www.semanticscholar.org/paper/Gender-Shades%3A-Intersectional-Accuracy-Disparities-Buolamwini-Gebru/18858cc936947fc96b5c06bbe3c6c2faa5614540. [Buolamwini & Gebru, *Gender Shades*]. There is also a recursive relationship between how algorithms are used by public safety actors and their impacts, because those deploying systems such as FRT have the discretion to make key decisions including inclusion criteria for watchlists and therefore who constitutes a 'threat': Pete Fussey, Bethan Davies & Martin Innes, "'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing", (2021) 61:2 *The British Journal of Criminology* 325, online: https://doi.org/10.1093/bjc/azaa068.

[47] Robertson, Khoo & Song, *To Surveil and Predict* at 25.

[48] See e.g., Garvie, *Garbage In, Garbage Out*; Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown, 2016); Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Oxford: Polity, 2019); Ngozi Okidegbe, "The Democratizing Potential of Algorithms?" (2022) 53:4 *Conn LR* 739.

[49] See e.g., Scot Wortley and Akwasi Owusu-Bempah, "Race, police stops, and perceptions of anti-Black police discrimination in Toronto, Canada over a quarter century" (2022) *Policing: An International Journal*, online: https://www.emerald.com/insight/content/doi/10.1108/PIJPSM-11-2021-0157/full/html; John McKay, "Systemic Racism in Policing in Canada: Report of the Standing Committee on Public Safety and National Security" (2021), online: *Standing Committee on Public Safety and National Security* https://www.ourcommons.ca/Content/Committee/432/SECU/Reports/RP11434998/securp06/securp06-e.pdf; Scott Clark, "Overrepresentation of Indigenous People in the Canadian Criminal Justice System: Causes and Responses" (2019), online: *Minister of Justice and Attorney General of Canada* https://www.justice.gc.ca/eng/rp-pr/jr/oip-cjs/oip-cjs-en.pdf; Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham: Duke University Press, 2015).

[50] Adjab et al*, Past, Present, and Future.*

[51] *Ibid*.

[52] "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software" (19 December 2019), online: *National Institute of Standards and Technology* www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[53] See e.g., Kristen Thomasen et al, "Submission to the Toronto Police Services Board's Use of New Artificial Intelligence Technologies Policy – LEAF and The Citizen Lab" (20 December 2021) online (pdf): *Social Science Research Network* papers.ssrn.com/sol3/papers.cfm?abstract_id=3989271;
Kristen Thomasen & Suzie Dunn, "Reasonable Expectations of Privacy in the Era of Drones and Deepfakes: Examining the Supreme Court of Canada's Decision in *R v Jarvis*" in Jane Bailey et al, eds, *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Bingley, UK: Emerald Publishing, 2021).

[54] Buolamwini & Gebru, *Gender Shades*; Deborah Inioluwa Raji & Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI" *AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, January 2019), online (pdf): dam-prod.media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf.

[55] Maggie Zhang, "Google Photos Tags Two African-Americans as Gorillas Through Facial Recognition Software", *Forbes* (1 July 2015), online: www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/; Ryan Mac, "Facebook Apologies After A.I. Puts 'Primate' Label on Video of Black Men", *The New York Times* (3 September 2021), online: www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html.

[56] Alex Najibi, "Racial Discrimination in Face Recognition Technology" (24 October 2020), online (blog): *Science In The News, Harvard University* sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[57] Lisa Marshal, "Facial recognition software has a gender problem" (8 October 2019), online: *CU Boulder Today, University of Colorado Boulder* https://www.colorado.edu/today/2019/10/08/facial-recognition-software-has-gender-problem.

[58] Davies, Innes & Dawson, *An Evaluation*; Fussey & Murray, *Independent Report*. See also Pete Fussey, Bethan Davies & Martin Innes, "'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing" (2020) 61:2 Brit J Crim.

[59] Davies, Innes & Dawson, *An Evaluation* at 18.

[60] Samuel Tanner & Michael Mayer, "Police work and new 'security devices': a tale from the beat" (2015) 46(4) *Security Dialogue* 384.

[61] Christopher D O'Connor, "Thinking about police data: Analysts' perceptions of data quality in Canadian policing" (2021) 20:10 *Police J: Theory, Practice and Principles* 1.

[62] Fussey & Murray, *Independent Report* at 124.

[63] *Ibid*.

[64] *Ibid*.

[65] Kathleen Harris, "Speaker condemns 'racial profiling' of black visitors to Parliament Hill", *CBC* (19 February 2019), online: www.cbc.ca/news/politics/black-voices-racism-regan-1.5024623.

[66] *Ibid*.

[67] Olivia Stefanovich, "Nunavut MP Mumilaaq Qaqqaq says departure from Parliament not the end of her story", *CBC* (17 June 2021), online: http://www.cbc.ca/news/politics/mumilaaq-qaqqaq-parliament-departure-1.6068711 [Stefanovich, *Nunavut MP Mumilaaq departure*].

[68] Rachel Aiello and Ben Cousins, "'I have never self safe': Nunavut MP accuses parliamentary security of racial profiling in farewell speech", *CBC* (16 June 2021), online: www.ctvnews.ca/politics/i-have-never-felt-safe-nunavut-mp-accuses-parliamentary-security-of-racial-profiling-in-farewell-speech-1.5472774.

[69] Robertson, Khoo & Song, *To Surveil and Predict*.

[70] Kevin D Haggerty, "The unarticulated political appeals of security-related risk technologies" in Stacey Hannem, Carries Sanders, Christopher Schneider, Aaron Doyle & Tony Christensen, eds, *Security and Risk Technologies in Criminal Justice: Critical Perspectives* (Canadian Scholars: Toronto, 2019) ix–1.

[71] Richard V Ericson & Kevin D Haggerty, *Policing the Risk Society* (Toronto: University of Toronto Press, 1997); Kristie Ball & Frank Webster, *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* (London: Pluto Press, 2003) [Ericson & Haggerty, *Policing the Risk Society*].

[72] Yuan Stevens & Ana Brandusescu, "Weak privacy, weak procurement: The state of facial recognition in Canada", *Centre for Media, Technology, & Democracy* (6 April 2021), online: www.mediatechdemocracy.com/work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada.

[73] Simon Egbert & Matthias Leese, *Criminal Futures* (London: Routledge, 2020).

[74] Lucia Zedner, "Pre-crime and post-criminology?", *Theoretical Criminology* 11:2 (1 May 2007) 261, online: doi.org/10.1177/1362480607075851. Pre-crime is introduced by Philip K. Dick's science fiction novel and made famous by Steven Spielberg's rendition, *Minority Report*.

[75] Johana Bhuiyan, "LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws", The Guardian (8 November 2021), online: www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform.

[76] See e.g., Wendy Hui Kyong Chun, *Discriminating Data: Correlation, Neighborhoods, and the New Politics of Recognition* (Cambridge, MA: MIT Press, 2021); Chris Gilliard, "Crime Prediction Keeps Society Stuck in the Past", *Wired* (2 January 2022), online: www.wired.com/story/crime-prediction-racist-history/; Kathleen McGrory & Neil Bedi, "Targeted", *Tampa Bay Times* (2 September 2020), online: projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/; Olivia Solon and Cyrus Farivar, "Predictive policing strategies for children face pushback" *NBC News* (6 June 2021), online: www.nbcnews.com/tech/tech-news/predictive-policing-strategies-children-face-pushback-n1269674.

[77] See e.g., the international Ban the Scan movement co-led by experts such as Matt Mahmoudi of Amnesty International and the Surveillance Technology Oversight Project (led by Albert Fox Cahn) among others: "Ban the Scan", *Amnesty International*, online: https://banthescan.amnesty.org/; the European movement called ReclaimYourFace facilitated by numerous civil society organizations including AccessNow, AlgorithmWatch, Article 19, EDRi, Privacy International, and numerous others: "About the movement", *ReclaimYourFace*, online: https://reclaimyourface.eu/the-movement/; as well as various more local campaigns in places such as the U.S. and beyond led by organizations like the Algorithmic Justice League, Electronic Frontier Foundation, and Fight for the Future: "About", *Algorithmic Justice League*, online: https://www.ajl.org/about; "Street-Level Surveillance", *Electronic Frontier Foundation*, online: https://www.eff.org/pages/face-recognition; "Ban Facial Recognition", *Ban Facial Recognition*, online: https://www.banfacialrecognition.com/. There is also a growing movement in Canada to prohibit the use of FRT or at the very least explicitly legislate its potential use by experts and civil society actors in order to address its harms, see e.g., efforts on privacy and surveillance led by Brenda McPhail at the CCLA: "Facial Recognition", *Canadian Civil Liberties Association*, online: https://ccla.org/our-work/privacy/surveillance-technology/facial-recognition/; efforts on face recognition particularly led by Tim McSorley at the ICMLG, "Open Letter: Canadian Government Must Ban Use of Facial Recognition by Federal Law Enforcement, Intelligence Agencies", (8 July 2020) *International Civil Liberties Monitoring Group*, online: https://iclmg.ca/facial-recognition-letter/; as well as efforts facilitated by experts such as Suzie Dunn, Kristen Thomasen, Kate Robertson, Christopher Parsons, Rosel Kim, and numerous others on behalf of the Women's Legal Education & Action Fund and Citizen Lab: Kristen Thomasen et al, "Submission to the Toronto Police Services Board's Use of New Artificial Intelligence Technologies Policy – LEAF and The Citizen Lab" (20 December 2021) online (pdf): *Social Science Research Network* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3989271.

[78] Robertson, Khoo & Song, *To Surveil and Predict*.

[79] Michelle McQuigge,"Canadian police using controversial 'predictive policing' tools, report finds" *Global News* (1 September 2020), online: globalnews.ca/news/7309391/canada-police-predictive-tools-report/.

[80] Justin Ling, "Saskatoon police spearheading new, high-tech way to look at missing person cases" *The Globe and Mail* (17 January 2020), online: www.theglobeandmail.com/canada/article-saskatoon-police-spearheading-new-high-tech-way-to-look-at-missing/; Nathan Munn, "Police in Canada are tracking people's 'negative' behaviour in a 'risk' database", *Vice* (27 February 2019), online: www.vice.com/en/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a-risk-database.

[81] Mike Maguire & Tim John, "Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK", *Policing and Society* 16 :1 (20 August 2006) 67, online: doi.org/10.1080/10439460500399791; David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2002); Ericson & Haggerty, *Policing the Risk Society*.

[82] Carrie B Sanders & Debra Langan, "New public management and the extension of police control: community safety and security networks in Canada", *Policing and Society* 29:5 (29 January 2018) 566, online: doi.org/10.1080/10439463.2018.1427744.

[83] Kelly A Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York: NYU Press, 2011).

[84] Israel, *Facial Recognition at a Crossroads*.

[85] Robertson, Khoo & Song, *To Surveil and Predict*.

[86] See e.g., Luke Stark, "Facial recognition is the plutonium of AI" (April 2019), online: *ACM XRDS* https://xrds.acm.org/article.cfm?aid=3313129 on the bigger picture dangers of failing to regulate FRT. See also Office of the Privacy Commissioner of Canada, *Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology,* Catalogue No IP54-110/2021E-PDF (Ottawa: Privacy Commissioner, 2021) [Privacy Commissioner, *Special report to Parliament*]; Yuan Stevens, "Now You See Me? Advancing Data Protection and Privacy for Police Use of Facial Recognition in Canada" (October 2021), online: *Cybersecure Policy Exchange* www.cybersecurepolicy.ca/now-you-see-me; Yuan Stevens & Sonja Solomun, "Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act" (17 February 2021), online: *Cybersecure Policy Exchange* www.cybersecurepolicy.ca/frt-privacy-act [Stevens & Solomun, *Facing the Realities of Facial Recognition Technology*].

[87] Joanne Laucius, "Security on Parliament Hill has ramped up since Zehaf-Bibeau attack in 2014", *Ottawa Citizen* (24 July 2018), online: ottawacitizen.com/news/local-news/security-on-parliament-hill-has-ramped-up-since-zehaf-bibeau-attack-in-2014.

[88] *Ibid*.

[89] "RCMP step up video surveillance of Parliament Hill", *CBC* (7 December 2013), online: www.cbc.ca/news/canada/rcmp-step-up-video-surveillance-of-parliament-hill-1.2455519.

[90] *Ibid*.

[91] Jim Bronskill, "Crowd flows, camera coverage being studied to bolster Parliament Hill Security", *CTV News* (26 June 2017), online: ottawa.ctvnews.ca/crowd-flows-camera-coverage-being-studied-to-bolster-parliament-hill-security-1.3477187.

[92] With this said, a more restrictive use case of FRT in terms of deployment may be correlated with the level of restriction placed on rights.

[93] "Facing the Camera Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales" *Surveillance Camera Commissioner* (November 2020), online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf.

[94] Library of Parliament, "Legislative Summary of Bill C-59: An act to implement certain provisions of the budget tabled in Parliament on April 21, 2015 and other measures", (12 May 2015) *Parliament of Canada*, online: https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/412C59E [Library of Parliament, *Legislative Summary of Bill C-59*].

[95] "RCMP Security Posture, Parliament Hill, October 22, 2014: OPP Review & Recommendations March 2015 – Security Responsibilities" (March 2015), online: *Royal Canadian Mounted Police* www.rcmp-grc.gc.ca/en/rcmp-security-posture-parliament-hill-october-22-2014#sr.

[96] *Ibid*.

[97] *Ibid*.

[98] *Ibid*.

[99] "RCMP Security Posture, Parliament Hill, October 22, 2014: OPP Review & Recommendations March 2015 – Executive Summary" (March 2015), online: *Royal Canadian Mounted Police* www.rcmp-grc.gc.ca/en/rcmp-security-posture-parliament-hill-october-22-2014#exec [RCMP, *Executive Summary*].

[100] *Ibid*.

[101] *Ibid*.

[102] *Ibid*.

[103] *See* e.g., House of Commons, *Incident Response Summary* at 4 & 7-9 and RCMP, *Executive Summary*.

[104] *Parliament of Canada Act*, RSC 1985, c P-1 [*Parliament of Canada Act*]. The relevant provisions of the *Act* are found in sections 79.51-79.58, which can be found in **Appendix B.**

[105] The MOU was signed pursuant to section 79.55 of the *Act* in order to clarify relevant provisions of the law. The PPS has not made the MOU public. However, the *Ottawa Citizen* was able to obtain a copy of the MOU in July 2015 and has shared a public version, which is found in **Appendix C**. At the time of writing, we received confirmation from the PPS that this version of the MOU is up-to-date. See Glen McGregor, "The Gargoyle: Agreement confirms Blaney responsible for Hill security", *Ottawa Citizen* (2 June 2020), online: ottawacitizen.com/news/politics/the-gargoyle-agreement-confirms-blaney-responsible-for-hill-security.

[106] In February 2015, a motion was adopted by the House of Commons and the Senate recognizing the "necessity of fully integrated security throughout the Parliamentary precinct and the grounds of Parliament Hill." (See House of Commons, *Incident Response Summary* at 8.) This motion was adopted roughly three months after the attack. There were also only roughly six months between the attack on Parliament Hill in late October 2014 and the introduction of the amendments to the Act in early May 2015. See e.g., Library of Parliament, Legislative Summary of Bill C-59.

[107] "Memorandum of Understanding between the Speaker of the Senate, The Speaker of the House of Commons, The Minister of Public Safety and Emergency Preparedness, and the Commissioner of the RCMP" (2015) para 2, online: *Scribd* www.scribd.com/document/272852261/PPS-MOU-en-Final [*Memorandum of Understanding*].

[108] However, paragraph 10 of the MOU states that PPS's Director is "responsible for planning, directing, managing and controlling operational parliamentary security, including members of the RCMP, House of Commons and Senate Protective Services."

[109] *Memorandum of Understanding* at para 11b.

[110] *Criminal Code*, RSC 1985, c C-46, s 494; *Trespass to Property Act,* RSO 1990, c T-21, s 9.

[111] *Ibid*.

[112] *Ibid*.

[113] *Parliament of Canada Act*, s 79.51.

[114] *Ibid*.

[115] *Ibid*.

[116] André Gagnon & Marc Bosc, "The Physical Administrative Setting: The Parliament Buildings and Grounds" in André Gagnon & Marc Bosc, eds, *The House of Commons Procedure and Practice*, 3rd edition (Ottawa: House of Commons, 2017) [Gagnon & Bosc, *House of Commons Procedure and Practice*].

[117] *Memorandum of Understanding* at para 11a.

[118] *Ibid* at para 11c.

[119] *Ibid* at para 11d.

[120] *Parliament of Canada Act,* s 79.53(1). An organizational chart can also be found here: "Organization Chart" online (pdf): *Parliamentary Protective Service* pps.parl.ca/wp-content/uploads/2019/06/PPS-SPP-organization-chart-organigramme-062019-1.pdf.

[121] *Parliament of Canada Act*, s 79.52(2).

[122] *Memorandum of Understanding* at para 7a.

[123] *Parliament of Canada Act*, s 79.54(2).

[124] *Ibid*, ss 79.52(2), 79.55(1). In 2021, the Minister of Emergency Preparedness and Public Safety became two separate ministers: the Minister of Public Safety and the Minister of Emergency Preparedness. The RCMP now reports to the Ministry of Public Safety, which is why we refer only to this ministry in this report.

[125] *Parliament of Canada Act*, s 79.54(2); *Memorandum of Understanding* at preamble and para 7b, emphasis added.

[126] *Parliament of Canada Act*, s 79.56(2).

[127] *Memorandum of Understanding* at para 5.

[128] *Royal Canadian Mounted Police Act*, RSC 1985, c R-10, s 5.

[129] *Memorandum of Understanding* at para 4.

[130] *The Constitution Act, 1982, Schedule B to the Canada Act* 1982 (UK), 1982, c 11, https://canlii.ca/t/ldsx, s. 18; Warren J Newman, "Parliamentary Privilege, the Canadian Constitution and the Courts" (2008) 39:3 Ottawa L Rev 575 at 599, citing *New Brunswick Broadcasting Co v Nova Scotia (Speaker of the House of Assembly)*, [1993] 1 SCR 319, 1993 CanLII 153 (SCC), [*New Brunswick Broadcasting Co v Nova Scotia*].

[131] Warren J Newman, "Parliamentary Privilege, the Canadian Constitution and the Courts" (2008) 39:3 Ottawa L Rev 575. See also: Warren J Newman, "The Rule of Law, The Separation of Powers and Judicial Independence in Canada" in Peter Oliver, Patrick Macklem & Nathalie Des Rosiers, eds, *Oxford Handbook of the Canadian Constitution* (New York: Oxford University Press, 2017). For more on other privileges and immunities available, see e.g., Philippe Lagassé, "Defence intelligence and the Crown prerogative in Canada" (2021) 64:4 *Canadian Public Administration* 539, online: doi.org/10.1111/capa.12439.

[132] See e.g., Senate, *Parliamentary Privilege: Then and Now, Report of the Standing Committee on Rules, Procedures and the Rights of Parliament* (June 2019) (Chair: Hon Leo Housakos) [Senate, *Parliamentary Privilege*]. See also: Gagnon & Bosc, *House of Commons Procedure and Practice*.

[133] *Canada v Vaid,* Joseph Maingot, *Parliamentary Immunity in Canada (*Toronto: Lexis Nexis: 2016), *Chagnon v Syndicat de la function publique et parapublique du Québec*, 2018 SCC 39; *Singh c Attorney General of Quebec*, 2018 QCCA 257; Evan Fox-Decent, "Parliamentary Privilege, Rule of Law and the Charter after the Vaid Case" (Autumn 2007) *Canadian Parliamentary Rev* 27 at 35.

[134] Gagnon & Bosc, *House of Commons Procedure and Practice* citing *Vaid* at para 40.

[135] Senate, *Parliamentary Privilege.*

[136] *Parliament of Canada Act*, ss. 79.53(1), 79.53(1). A related provision in the MOU includes para 7(a), which provides that "the authority for security of the Parliamentary precinct is vested in the Speaker of the Senate and the Speaker of the House of Commons, as the custodians of the privileges, rights, immunities, and powers on behalf of their respective Houses and of the members of those Houses, as per the Constitution of Canada and the *Parliament of Canada Act*."

[137] The PPS could be seen as inheriting the parliamentary privilege afforded to the security services previously run by the House of Commons and the Senate. See e.g., Gagnon & Bosc, *House of Commons Procedure and Practice* at ch 3.; Maingot, *Parliamentary Immunity in Canada* at 155.

[138] Senate, *A Matter of Privilege: A Discussion Paper on Canadian Parliamentary Privilege in the 21st Century, Interim report of the Standing Committee on Rules, Procedures, and the Rights of Parliament* (June 2015) (Chair: Hon Vernon White) at 51 [Senate, *A Matter of Privilege*]. See also *Canada (Board of Internal Economy) v Boulerice,* 2019 FCA 33 at 66.

[139] Senate, *A Matter of Privilege* at 53.

[140] *Canada v Vaid*.

[141] See *New Brunswick Broadcasting Co v Nova Scotia*.

[142] See *Singh c Attorney General of Quebec*.

[143] *R v Behrens et al*, 2004 ONCJ 327.

[144] *Ibid*.

[145] *Parliament of Canada Act*, s 79.58; *Memorandum of Understanding* at para 11.

[146] House of Commons, Standing Committee on Procedure and House Affairs, *Evidence*, 42-1, No 57 (9 May 2017) 1005-1010 (Mr David Christopherson and Mr Andre Barnes),1005-1010.

[147] *Ibid.*

[148] Additionally, parliamentary privilege may not necessarily apply to certain actions of the PPS if its members act upon instructions from the executive branch in a way that exceeds the jurisdiction given to the PPS by the legislative branch, including decisions made as they relate to the use of FRT. This is because the executive branch cannot benefit from parliamentary privilege. See e.g., John R Richard, "Separation of Powers: The Canadian Experience" (2009) 47:4 Duq L Rev 731 at 731 and 739-741; Peter W Hogg, *Constitutional Law of Canada* (Toronto: Thomson Carswell, 2007).

[149] Senate, *Parliamentary Privilege*; Gagnon & Bosc, *House of Commons Procedure and Practice* at s 3 ("Individual Privileges").

[150] *Ibid*. Proceedings in the House of Commons and the Senate are covered by a bundle of parliamentary privileges that are recognized as necessary for parliamentarians and the legislature to conduct their functions. For individual parliamentarians, freedom of speech is arguably one of the most important privileges. This privilege is rooted in parliament's autonomy and the ability of parliamentarians to contribute freely to parliamentary debates.

[151] Stefanovich, *Nunavut MP Mumilaaq departure*; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (New York: St. Martin's Press. 2018).

[152] The immediate disposal of facial templates collected when they do not result in alerts could potentially address the risk that parliamentarians' locations could be tracked.

[153] For more on the location-based aspects of privacy, see e.g., Teresa Scassa

& Anca Sattler, "Location-Based Services and Privacy" (2011) 9:2 *CJLT* 99.

[154] "Data at Your Fingertips Biometrics and the Challenges to Privacy" (February 2011), online: *Office of the Privacy Commissioner of Canada* www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/. [Privacy Commissioner, *Data at Your Fingertips*].

[155] Privacy Commissioner, *Special report to Parliament.*

[156] *International Covenant on Civil and Political Rights*, GA Res 2200A(XXI), UNGAOR, 21st Sess (1966), art 17(1).

[157] "Draft privacy guidance on facial recognition for police agencies" (2021) at para 12, online: *Office of the Privacy Commissioner* www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/ [Privacy Commissioner, *Draft privacy guidance*]; Jane Bailey, "Towards An Equality-Enhancing Conception of Privacy" (2008) 31:2 *Dal LJ* 267.

[158] Privacy Commissioner, *Draft privacy guidance* at para 9.

[159] 'Government institutions' in the *Privacy Act* refers to (a) any department or ministry of state of the Government of Canada, or any body listed in the *Act*'s schedule, as well as (b) any parent Crown corporation and such corporation's wholly-owned subsidiaries. *Privacy Act*, RSC 1985, c P-21, s 3.

[160] Privacy Commissioner, *Draft privacy guidance* at para 50.

[161] See e.g., "Section 1 – Reasonable limits", *Government of Canada* (April 14, 2022), online: https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art1.html.

[162] This is despite the fact that parliamentary privilege could potentially be used to shield the use of FRT from judicial review; and the PPS may not fall under the *Privacy Act*'s definition of 'government institution'.

[163] Privacy Commissioner, *Draft privacy guidance* at para 55.

[164] *Privacy Act*, s 4.

[165] Privacy Commissioner, *Draft privacy guidance* at para 55.

[166] *Ibid*.

[167] Privacy Commissioner, *Special report to Parliament* at para 22

[168] Notably, the RCMP initially told the OPC that it had not used Clearview AI, but admitted to using the technology only after news reports revealed that the RCMP was one of Clearview AI's clients. See Privacy Commissioner, *Special report to Parliament* at para 10.

[169] Privacy Commissioner, *Joint investigation*.

[170] *Ibid*; Privacy Commissioner, *Special report to Parliament.*

[171] Privacy Commissioner, *Special report to Parliament.*

[172] Privacy Commissioner, *Draft privacy guidance* at para 56; Privacy Commissioner, *Data at Your Fingertips*. While a necessity test is not the legislated standard for examinations under s. 4 of the *Privacy Act* (see e.g., *Canada (Union of Correctional Officers) v Canada (Attorney General)*, 2019 FCA 212), these four considerations guide the OPC's investigations under the *Privacy Act*, thereby ensuring that the interpretations of the law develop in a manner that is consistent with the *Charter*: *Jones v Tsige*, 2012 ONCA 32, aff'd *RWDSU v Dolphin Delivery Ltd*, [1986] 2 SCR 573, 1986 CanLII 5 (SCC).

[173] Privacy Commissioner, *Draft privacy guidance* at para 57; "Office of the Privacy Commissioner Compliance Monitoring of Statistics Canada's Financial Transactions Project and Credit Agency Data Project: Final Report" (3 May 2021), online: *Office of the Privacy Commissioner of Canada* www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2020-21/pa_20210503_sc/ [Privacy Commissioner, *Statistics Canada's Financial Transactions: Final Report*].

[174] "Video surveillance of employees vs. right to privacy – a delicate balance: Complaint under the Privacy Act" (last modified 10 December 2015) at para 19, online: *Office of the Privacy Commissioner of Canada* www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2014-15/pa_20141113/ [Privacy Commissioner, *Video surveillance of employees: Complaint*].

[175] "Privacy Commissioner releases finding on video surveillance by RCMP in Kelowna" (4 October 2001), online: *Office of the Privacy Commissioner of Canada* web.archive.org/web/20220107115042/https://www.priv.gc.ca/en/opc-news/news-and-announcements/2001/02_05_b_011004/ [Privacy Commissioner, *Finding on video surveillance by RCMP*].

[176] Privacy Commissioner, *Draft privacy guidance* at para 57.

[177] Privacy Commissioner, *Data at Your Fingertips*.

[178] Privacy Commissioner, *Special report to Parliament*.

[179] Privacy Commissioner, *Draft privacy guidance* at para 57.

[180] Privacy Commissioner, *Special report to Parliament* at para 19.

[181] Privacy Commissioner, *Draft privacy guidance* at para 57.

[182] Stevens & Solomun, *Facing the Realities of Facial Recognition Technology*; Privacy Commissioner, *Draft privacy guidance* at para 57. There are also calls by privacy experts such as Teresa Scassa for the implementation of privacy laws that are grounded in a human rights approach: Teresa Scassa, "A Human Rights-Based Approach to Data Protection in Canada" in Dubois and Florian Martin-Bariteau, eds, *Citizenship in a Connected Canada: A Research and Policy Agenda* (Ottawa: University of Ottawa Press, 2020) 173.

[183] Privacy Commissioner, *Video surveillance of employees: Complaint* at para 19.

[184] "Global Affairs Canada fails to demonstrate its authority to collect the personal information contained in diplomatic passports: Complaint under the Privacy Act" (29 March 2019) at para 13, online*: Office of the Privacy Commissioner of Canada* www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2018-19/pa_20190329_gac/ [Privacy Commissioner, *Global Affairs fails to demonstrate its authority: Complaint*].

[185] Privacy Commissioner, *Draft privacy guidance* at para 58.

[186] *Privacy Act*, s 6(2).

[187] Privacy Commissioner, *Finding on video surveillance by RCMP*; *Privacy Act*, s 4.

[188] Privacy Commissioner, *Finding on video surveillance by RCMP.*

[189] *Privacy Act*, ss 7-8.

[190] Privacy Commissioner, *Draft privacy guidance* at para 59.

[191] *Ibid* at para 59.

[192] *Ibid* at para 60.

[193] *Ibid*.

[194] *Ibid*.

[195] *Ibid* at paras 64-69.

[196] Treasury Board Secretariat, Directive on Automated Decision-Making (Ottawa: Treasury Board Secretariat, 2019), online: *Treasury Board Secretariat* https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592; Teresa Scassa, "Administrative Law and the Governance of Automated Decision Making: A Critical Look at Canada's Directive on Automated Decision Making" (2021) 54 UBC L Rev 251 at 281 [Scassa, *Administrative Law and the Governance of Automated Decision Making*].

[197] Michele Loi et al, "Automated Decision-Making Systems in the Public Sector" (2021), online (pdf): *Algorithm Watch* algorithmwatch.org/en/wp-content/uploads/2021/09/2021_AW_Decision_Public_Sector_EN_v5.pdf. This civic engagement work should draw on best practices in order to be meaningful, and should not amount to what Sieber and Brandusescu have helpfully referred to as "performative empowerment." See Renee Sieber & Ana Brandusescu, "Civic Empowerment in the Development and Deployment of AI Systems" (2021) online, *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4104593. See also Dallas Hill, Christopher O'Connor & Andrea Slane, "Police Use of Facial Recognition Technology: The Potential for Engaging the Public Through Co-Constructed Policy-making" (2022) *Int J of Police Science & Management*, online: https://doi.org/10.1177/14613557221089558.

[198] *Memorandum of Understanding* at para 11b.

[199] Privacy Commissioner, *Video surveillance of employees: Complaint.*

[200] *Ibid*, at paras 19, 21.

[201] *Ibid*, at para 19.

[202] Privacy Commissioner, *Statistics Canada's Financial Transactions: Final Report*.

[203] Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the way forward*, (Special Report), Catalogue No IP54-110/2021E-PDF (Ottawa: Privacy Commissioner, 10 June 2021) [Privacy Commissioner, *Police use of Facial Recognition Technology in Canada: Special Report*]. The OPC has also come to this conclusion regarding the use of CCTV: Privacy Commissioner, *Finding on video surveillance by RCMP*.

[204] Privacy Commissioner, *Police use of Facial Recognition Technology in Canada: Special Report*, see especially paras 26-27.

[205] The use of the photos in the case of the RCMP involved scraping the images from the web, yet the creation of watchlists without people's consent can happen in many other ways. The use of photos without consent for training could be implicated. See e.g., Israel, *Facial Recognition at a Crossroads* at 52-57.

[206] Privacy Commissioner, *Police use of Facial Recognition Technology in Canada: Special Report*.

[207] *Ibid*, at para 15.

[208] *Ibid*, at para 18.

[209] Bruce Schneier, "Scaring People into Supporting Backdoors" (12 December 2019), online (blog): *Schneier on Security* www.schneier.com/blog/archives/2019/12/scaring_people_.html.

[210] David Lyon, *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination* (London: Routledge, 2002).

[211] Privacy Commissioner, *Draft privacy guidance.*

[212] Privacy Commissioner, *Global Affairs fails to demonstrate its authority: Complaint.*

[213] *Privacy Act*, s 6(2).

[214] Privacy Commissioner, *Draft privacy guidance* at para 58.

[215] Privacy Commissioner, *Statistics Canada's Financial Transactions: Final Report* at para 20.

[216] Israel, *Facial Recognition at a Crossroads* at 154.

[217] *R v Dyment*, [1988] 2 SCR 417 at para 34, 55 DLR (4th) 503.

[218] See e.g., "The ICRC biometrics policy" (15 October 2019) at ss 17.1-17.2, online: *International Committee of the Red Cross* www.icrc.org/en/document/icrc-biometrics-policy [ICRC, *ICRC biometrics policy*].

[219] *R v Spencer*, 2014 SCC 43.

[220] See e.g., Carmen-Cristina Cirlig, "Policing in national parliaments: How parliaments organise their security" (2021), online (pdf): *European Parliament* www.europarl.europa.eu/RegData/etudes/BRIE/2021/679072/EPRS_BRI(2021)679072_EN.pdf.

[221] *R v Dyment*.

[222] Privacy Commissioner, *Police use of Facial Recognition Technology in Canada: Special Report.*

[223] ICRC, *ICRC biometrics policy*; Ben Hayes & Massimo Marelli, "Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases" (2020), online (pdf) *AI Now Institute* https://ainowinstitute.org/regulatingbiometrics-hayes-marelli.pdf.

[224] *The Charter*, s 8.

[225] Nader Hassan et al, *Search and Seizure* (Toronto: Emond Publishing, 2021) ch 1 [Hassan et al, *Search and Seizure*].; Israel, *Facial Recognition at a Crossroads*.

[226] Robertson, Khoo & Song, *To Surveil and Predict*; Israel, *Facial Recognition at a Crossroads*; Hassan et al, *Search and Seizure,* ch 1.

[227] See also Moritz Buchi et al, "The chilling effects of algorithmic profiling: Mapping Issues" (2020) 26 *Computer L & Sec Rev* [Buchi et al, *The chilling effects of algorithmic profiling*].

[228] *R v Tessling*, 2004 SCC 67 at para 18.

[229] *R v Spencer*.

[230] *Ibid*, at para 44.

[231] See e.g., Teresa Scassa, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy" (2010) 7:1 *CJLT* 193.

[232] *R v Wise*, [1992] 1 SCR 527, 70 CCC (3d) 193; *R v Spencer*; *R v Jarvis* 2019 SCC 10.

[233] Hassan et al, *Search and Seizure*, at 51. See also: Robertson, Khoo & Song, *To Surveil and Predict* at 76.

[234] *R v Wise*.

[235] *Ibid*; Hassan et al, *Search and Seizure*, at 51.

[236] *Ibid.*

[237] Andrea Slane, "Privacy and Civic Duty in R v Ward: Right to Online Anonymity and the Charter-Compliant Scope of Voluntary Cooperation with Police Requests (2013) 39:1 *Queen's LJ* 301.

[238] *R v Spencer*.

[239] *Ibid*; Ana Qarri, "Bringing Section 8 Home: An Argument in Favour of Recognizing a Reasonable Expectation of Privacy in Metadata Collected from Smart Home Devices" (2022) 19 *CJLT* 457.

[240] Individuals do not lose their reasonable expectation of privacy simply because other people know about what they are doing, what are they protesting, etc.: See e.g., *R v Duarte*, [1990] 1 SCR 30, 65 DLR (4th) 240.

[241] See e.g., *R v Aubrey*, 2022 ONSC 635; *R v Yu*, 2019 ONCA 942 at paras 128–129 [*R v Yu*].

[242] *R v Yu*, at 128–129.

[243] Anne Dance, "Negotiating Public Space on Canada's Parliament Hill: Security, Protests, Parliamentary Privilege, and Public Access" (2014) 48: 2 *Journal of Canadian Studies* 169 at 176-178 [Dance, *Negotiating Public Space on Canada's Parliament Hill*].

[244] *The Charter*, s 2.

[245] *Irwin Toy Ltd. v Quebec (Attorney General),* [1989] 1 SCR 927, 58 DLR (4th) 577.

[246] Robert J Sharpe & Kent Roach, *The Charter of Rights and Freedom* (Irwin Law: Toronto, 2021) at 150-152, 177-178 [Sharpe & Roach*, The Charter*].

[247] *The Charter*, s 1.

[248] *Canadian Broadcasting Corp v Canada (Attorney General)*, 2011 SCC 2 at 37*; Montréal (City) v 2952-1366 Québec Inc*, 2005 SCC 62 at 72 [*Montréal (City) v 2952-1366 Québec Inc*].

[249] *Montréal (City) v. 2952-1366 Québec Inc; Committee for the Commonwealth of Canada v Canada*, [1991] 1 SCR 139, 77 DLR (4th) 385.

[250] *Ibid*.

[251] On top of this, it could be possible to argue that the exercise of free expression in the parliamentary context should include the ability to visit a Member of Parliament or to participate in parliamentary proceedings.

[252] "Organizing an event on Parliament Hill? Start Here!" online: *Parliament of Canada* hill-colline.parl.ca/en/ [Parliament of Canada, *Organizing an event on Parliament Hill?].*

[253] Dance, *Negotiating Public Space on Canada's Parliament Hill*.

[254] "The Parliament of the Federal Republic of Germany", online: *German Bundestag* www.bundestag.de/en/; "New Zealand Parliament" online: *New Zealand Parliament* www.parliament.nz/en.

[255] See e.g., *Weisfeld v Canada*; *Public Works Nuisances Regulations*, CRC, c 1365 (2022).

[256] "General Rules for the Use of Parliament Hill" (last modified 22 October 2018), online (pdf): *Parliament of Canada* http://hill-colline.parl.ca/pdf/CUPH-Rules-e.pdf.

[257] Parliament of Canada, *Organizing an event on Parliament Hill?.*

[258] Dance, *Negotiating Public Space on Canada's Parliament Hill* at 181.

[259] Buchi et al, *The chilling effects of algorithmic profiling*, s 3.2.

[260] Jon Penney "Chilling effects: Online surveillance and Wikipedia use" (2016) 13:1 *BTLJ* 117; Jonathon W Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017) 6:2 *Internet Policy Review* 22.

[261] Buchi et al, *The chilling effects of algorithmic profiling*, s 3.2.

[262] Jon Penney, "Understanding Chilling Effects" (2021) *Minn L Rev* 101.

[263] "Section 15 – Equality Rights" (last modified 14 April 2022), online: *Government of Canada* www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art15.html .

[264] *Ibid*; Sharpe & Roach, *The Charter* at 307.

[265] *Fraser v Canada (Attorney General),* 2020 SCC 28 [*Fraser v Canada*]; Carissima Mathen, "Equality Before the Charter: Reflections on Fraser v Canada" (15 January 2022) [forthcoming in *SCLR*], online (pdf): dx.doi.org/10.2139/ssrn.4009862.

[266] Sharpe & Roach, *The Charter* at 315; Jane Bailey, "Towards An Equality-Enhancing Conception of Privacy", (2008) 31(2) *Dalhousie Law Journal* 267 at 288.

[267] *Fraser v Canada,* at paras 27, 81.

[268] Reva Schwartz et al, "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence" (March 2022) at 3, online(pdf): *National Institute of Standards and Technology (NIST)* nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf [Schwartz et al, *Standard for Artificial Intelligence*]; Natasha Singer & Cade Metz, "Many Facial-Recognition Systems are Biased, Says US Study" *The New York Times* (19 December 2019), online: www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

[269] Schwartz et al, *Standard for Artificial Intelligence* at 5.

[270] Buolamwini & Gebru, *Gender Shades* at 1-15.

[271] Kimberle Crenshaw, "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics" (1989) 1989:1 *U Chicago Legal F* 139.

[272] Jeff Larson et al, "How We Analyzed the COMPAS Recidivism Algorithm*" ProPublica* (23 May 2016), online: www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

[273] Alina Kochling & Marius Claus Wehner, "Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development" (2020) 13 *Business Research* 795, online: link.springer.com/article/10.1007/s40685-020-00134-w#Sec11.

[274] Kashmir Hill, "Another Arrest and Jail Time, Due to a Bad Facial Recognition Match: A New Jersey man was accused of shoplifting and trying to hit an officer with a car. He is the third known Black man to be wrongfully arrested based on face recognition", *The New York Times* (6 January 2021), online: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[275] See e.g., Khari Johnson, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives", *Wired* (7 March 2022), online: www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.

[276] *Ewert v Canada*, 2018 SCC 30.

[277] Scassa, *Administrative Law and the Governance of Automated Decision-Making*.

[278] Israel, *Facial Recognition at a Crossroads* at 116.

[279] *Bridges v CCSW Police & Information Commissioner.*

[280] Vivek Krishnamurthy, "AI and Human Rights Law" in Florian Martin-Bariteau & Teresa Scassa, eds, *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis, 2021).