Maaz Saad

Dr. Theresa Miedema

MBAI 5200G

12 December 2022

Major Case Study – Algorithmic Policing in Canada

Algorithmic policing involves the use of algorithms and various forms of artificial intelligence technology to aid in law enforcement, and this type of policing has become increasingly popular in Canada in recent years. While this type of policing can have numerous potential benefits, such as more efficient use of resources, improved accuracy in identifying potential suspects, and lower costs, it also raises important ethical and legal concerns that need to be addressed.

In this paper, we will try to understand how algorithmic policing works in Canada and how law enforcement agencies are adopting this technology into their daily practices. After developing an understanding of the concept of algorithmic policing, we will shift our focus to one of the key ethical principles at stake in algorithmic policing, which is the principle of trust between the people and the government. In Canada, the government has a duty to protect the rights and freedoms of its citizens, and this includes ensuring that law enforcement practices are fair and transparent (Justice). However, the use of algorithms in policing can create a lack of trust if the public is not fully informed about how these algorithms work and what data they use. So, our paper will focus on the necessity of trust between the government and its citizens.

Additionally, Canadian law has an important role to play in the ethical use of algorithmic policing. The Charter of Rights and Freedoms, which is part of the Canadian Constitution, guarantees certain rights and freedoms to all individuals, including the right to life, liberty, and security of the person (Justice). This means that any use of algorithms in policing must be consistent with these rights and must not unfairly target certain individuals or groups (Justice).

Algorithm policing in Canada can be divided into two categories. The first type is predictive policing, which includes location-focused policing and person-focused policing, and the second type is algorithmic surveillance technology (Kenyon). Predictive policing is essentially a type of machine learning model that takes into account historical data and predicts the probability of a criminal activity taking place (Kenyon). The model can predict the probability of a crime taking place in a certain area or neighborhood, and this type of prediction is location-focused (Kenyon). On the other hand, person-focused prediction means that the algorithm can predict the probability of a person committing a crime or engaging in some type of criminal activity (Kenyon). Secondly, algorithmic surveillance technologies do not effectively make predictions (Kenyon). Instead, they provide law enforcement officials with advanced surveillance and monitoring functions (Kenyon). This can be in the form of pattern recognition in license plate numbers or looking for potential malicious intent in a person's social media activity, and its most fascinating feature is its facial recognition ability to identify and match the faces of suspects in a large crowd or gathering (Kenyon).

Artificial intelligence is the first step towards a different future. Whether it's brighter or bleaker remains to be seen. AI will catapult us into this future despite its current challenges, such as safety, privacy, bias, and the issue of building a legal landscape surrounding AI due to its ever-evolving nature (Chatila et al. 14). It is necessary to develop a methodology to explain the

way an artificially intelligent system works to facilitate people's trust in the systems (Chatila et al. 14). Fortunately, there has been an increased effort in improving the ethical, societal, and legal implications of AI from all the top countries in the world (Chatila et al. 14). The term that can be adopted for this new generation of smarter and more intelligent AI systems is "Trustworthy AI" (Chatila et al. 14). And as the name suggests, the goal of trustworthy AI is to be lawful, ethical, and robust (Chatila et al. 14).

There is some misconception about this term, and people often assume that our goal with trustworthy AI is to build a model that can think and feel like a human and replace human jobs (Chatila et al. 15). That is certainly not the case. The true purpose of AI is to automate tasks that can help cut costs and save time. It should be simple enough for humans to trust this system, but the reason they don't is because these AI systems have shown bias towards minorities and people of color and come up with some truly bizarre conclusions. People don't need to trust AI systems. They need to trust that the people and organizations that built these models considered all possible variables and that these models are actually accurate (Chatila et al. 15). People still need to trust people at the end of the day.

People's trust in trustworthy AI can be achieved through publicly showcasing the impartiality of AI models prior to implementation to help build confidence that these models do not discriminate based on social, geographical, or ethnic status (Omrani et al. 3). AI models that are based on neural networks have been condemned due to their "black-box nature", which means that as the audience, you can only see the input and the output with no idea of the layers of modeling and analysis that happen within (Omrani et al. 2). Research has suggested that people will always prefer the advice they get from a human being as opposed to a computer system, even if the system's advice is much better than that of a human (Hobson et al. 3). So, in

order to reduce this apprehension towards AI systems, a number of small steps need to be taken by the government to improve the level of trust between humans and AI-powered solutions. In the section, we assessed what trust in AI means to the developers building them. In the next section, we will try to get an understanding of what it means for the public to trust an AI system, as both these perspectives are different and yet, very important to understand.

At this point, having learned about the aspects of an AI-powered policing model, it is imperative to critically assess these notions from the perspective of the general public. Trust between the government and the masses of the population is what maintains law and order and prevents chaos from ensuing. As a citizen of Canada, it would be hard for people with a criminal history to feel safe knowing that an algorithm is using person-focused policing methods to determine if they are likely to commit a crime anytime soon. It is the government's job to build a sense of trust between the public and their technological approach to policing to make people with a criminal background feel like they belong to society, especially when they have paid for their crimes either by paying fines or having done jail time.

The next level of building trust is even harder because this time the government needs to convince an entire or part of a municipality that location-focused algorithmic policing will not negatively impact their daily lives. By condemning a certain portion of a municipality as a high-risk area, the government is essentially alienating that part of their population and stating that they do not trust the people to act like decent citizens. These are ethical dilemmas that every police department that has adopted or wants to adopt algorithmic policing will need to consider if they truly want to build a relationship with their community.

Lastly, using facial recognition technology to recognize faces in a crowd against faces on a most wanted list or a terrorist watch list is an extremely risky order of business. This can have

dire and unforeseen consequences that can lead to violations of a person's right to be treated fairly, and police departments can face lawsuits and get tied up in litigation. Therefore, the accuracy and precision of AI models that are making decisions about human lives needs to be at their highest level.

Since the focus of our paper is algorithmic policing in Canada, it makes logical sense for us to glance over some of the law enforcement establishments within Canada that have embraced algorithmic policing or are in the process of doing so. The Vancouver Police Department currently utilizes location-focused algorithmic policing technologies to predict the likelihood of a break-and-enter happening in any area during any given two-hour period of a day and then ranks them by neighborhood (Kenyon). The Toronto Police Service has access to IBM's data mining and predictive modeling software but has yet to implement any location-focused algorithmic policing technologies into practice (Kenyon).

The Saskatoon Police Service has taken a different approach to the person-focused algorithmic capabilities of an AI system. Instead of tracking down potential criminals or surveilling repeat offenders, they decided to use this software to proactively identify potential victims, such as missing people, and hope to expand the software's capability to pursue at-risk individuals or people with mental illness (Kenyon). Moreover, the Ontario Ministry of the Attorney General is currently reviewing and assessing the viability of a pre-trial risk assessment tool that can help automate pre-trial detention, such as bail decisions (Kenyon).

As for algorithmic surveillance, police vehicles and highways in provinces such as Ontario, British Columbia, Alberta, and Quebec have been equipped with automated license plate readers to help track down stolen vehicles or track down cars that were recently seen at a crime scene (Kenyon). Furthermore, the Ontario Provincial Police is quite possibly surveilling

private chat rooms in the hopes of catching child predators and reducing cybercrimes against young children through the use of a tool known as the “ICAC Child Online Protection System” (Kenyon). As a final example, Calgary’s Police Service and Toronto’s Police Service currently use facial recognition technology to compare hand-drawn sketches or crime scene photos of potential suspects with their mug-shot databases (Kenyon).

All these examples are from actual police departments across Canada that use AI-powered tools to help them in their policing activities. On first glance, it may seem that the technology is smart enough to make the right choices and that the entire process is effortless with little to no room for error. That cannot be further from the truth. In February 2020, several law enforcement agencies across Canada were caught with their fingers in the cookie jar, with the cookie jar being a metaphor for the AI-powered toolbox that solves crimes while the police officers enjoy longer lunch breaks. These agencies used the contentious facial recognition tool Clearview AI, which trained its machine learning algorithms on roughly 3 billion photos of faces downloaded from the internet without the consent of the people (Kenyon). We started our research by arguing that for AI policing to be accepted nationwide, there needs to be a great deal of trust between law enforcement organizations and the public and using controversial software systems will not help build that trust.

Earlier in the paper, we touched upon the fact that we will be analyzing the processes and procedures of algorithmic policing in Canada from the perspective of the law, especially the Charter of Rights and Freedoms. In April 1982, Queen Elizabeth II signed the Canada Act in Ottawa (Justice). This act afforded Canada the right to have control over its constitution and “guaranteed the rights and freedoms in the Charter as the supreme law of the nation (Justice).”

Before we delve further into our study, it is crucial to understand why we need to re-examine the law from the perspective of algorithmic policing. The reasoning is simple. If a police officer were to infringe upon human rights obligation, the Canadian government would be responsible for taking judicial action or otherwise remedying the situation in favor of the affected party (Robertson et al. 70). In the same manner, if an AI-powered policing tool malfunctions and leads to a wrongful arrest or detention, the Canadian government will need to provide compensation for that error in judgement. Since the end goal is to incorporate algorithmic policing into regular policing, there cannot be separate laws for human law enforcement officers and algorithmic law administration. Therefore, it is wise to discern how the Charter safeguards people's rights against the negative elements of algorithmic policing.

In this next section, we shall look at the implications of algorithmic policing techniques on the rights afforded to Canadians through the Charter of Rights and Freedoms. These rights include: the right to privacy, the right to freedom of expression, peaceful assembly, and association, the right to equality and freedom from discrimination, the right to liberty and to be free from arbitrary detention, the right to due process, and the right to a remedy (Robertson et al. 69). Since, it is not feasible to cover every single one of these rights due to the nature of this study; we will focus solely on one's right to privacy. We will provide a description of the right to privacy and review how it protects Canadians, and we will examine the challenges that are faced while trying to uphold it in the light of algorithmic policing including looking at actual case examples from the recent past.

The right to privacy comes into play while examining AI policing tools due to the nature of the models and algorithms that power these tools (Robertson et al. 73). These models are built on the backbone of gigantic amounts of data collected from any number of sources (Robertson et

al. 73). This data includes personal information about people that they might not want to be used in a public setting. Therefore, it is imperative that precautionary measures are taken to protect the privacy of citizens because the data gathering, and analysis procedures linked to algorithmic policing may make the public feel vulnerable to privacy incursions (Robertson et al. 73). Without such measures that regulate how data is collected and processed, the risks to an individual's privacy might increase ten-fold to the point where they are unaware that they are being monitored or recorded (Robertson et al. 73). And this is the opposite of what the Canadian constitution preaches.

The Supreme Court of Canada has acknowledged that the protection of an individual's information is critical in today's digital society (Robertson et al. 74). And on that note, it is pertinent to mention that the Charter, under section 8, has recognized that unlawful incursions on a person's privacy communicate a poor representation of a free and democratic society (Robertson et al. 73). Simply collecting and processing data in an intelligent fashion is not enough, as unforeseen issues arise when we bring the concept of data sharing into play, that is, the sharing of confidential data between law enforcement agencies and government institutions or even the private sector (Robertson et al. 73). From this, we can establish the dire need for a regulatory body to oversee that institutions that use algorithmic techniques, do so in a manner that is not threatening to the privacy interests of society (Robertson et al. 73).

We need to circle back to the concept of data collection as it is not as straightforward and simple as it might seem. How and where the data is collected can make all the difference in a case. It is safe to say that algorithmic surveillance technologies are trained and tested on data sets obtained from public sources (Robertson et al. 75). But the term public information takes on a new meaning when law enforcement gets involved. According to R v Wise, [1992] 1 SCR 527;

R v Cole, 2012 SCC 3; R v Marakah, 2017 SCC 59; R v Jones, 2017 SCC 60, people cannot retain airtight control over their personal information forever (Robertson 75). However, it is reasonable for people to expect that their information will not be shared with law enforcement agencies (Robertson et al. 75).

Furthermore, on the ethics of data collection, section 8 of the Charter further claims that if law enforcement officers wish to leverage the private information of individuals for their investigations, they must have "reasonable grounds" that the information will more likely than not lead to an arrest or, at the very least, reveal the evidence of a crime (Robertson et al. 78). The reason behind this staunch stance is to impede fishing expeditions by law enforcement officials hoping for a Hail Mary (Robertson et al. 75).

For this next part, let us take into consideration a police database that has a multitude of data that was collected over several decades and was used for traditional policing practices (Robertson et al. 79). It is exciting to ponder over the legal implications of using this data that the police precincts already have as the training and testing sets for designing automated policing models (Robertson et al. 79). Expanding on this idea, let us connect the dots on what exactly this idea entails. Let us say, police officers responded to a criminal complaint about a theft in a grocery store. And as part of their statements, they noted down the store owner's personal information, such as their family size, family dynamics, medical history, monthly income, and a whole other list of variables that are not relevant to the theft but needed to be taken down as part of regular police procedure. Now, what will the legal implications be if that person's family size was used to train machine learning models? There is a case to be made that it is being done with the right intentions, and it might help the police notice patterns such as store owners with a family size of five or higher being fifteen percent more likely to get robbed. On the other hand,

information about a person's family should not be used in such a manner, especially when that person has not given their consent to be treated as data points.

Building upon the immense need for collecting data in an ethical and principled way, section 8 requires law enforcement officials to obtain a search warrant before they can investigate an individual's personal belongings (Robertson et al. 80). Similarly, an algorithmic policing model needs to be held to the same legal standards. For example, the Office of the Privacy Commissioner ruled in 2013 that the government's surveillance and collection of personal data from the Facebook page of Cindy Blackstock (an Indigenous rights activist) violated the Privacy Act (Robertson et al. 76). The AI-powered tool cannot use all publicly available data as evidence against one's wrongdoing. Humans need to define the parameters of the data that the AI model can utilize in accordance with what the Privacy Law states. So that the conclusions of the AI model can be decisively held up in a court of law.

In R v Patrick, the police collected evidence in an individual's garbage inside that individual's residential property through aerial means (Singh 8). The court concluded that Patrick had discarded his right to privacy as he had thrown out that object, and by doing so, he had let go of his right to the information contained in the trash, and the police were allowed to use it as evidence in the case (Singh 8). This opens up a wide range of questions that need to be considered while building AI models. Especially around what aspects of an individual's privacy can be circumvented to achieve evidence of wrongdoing and the degree of wittiness an algorithm can learn similar to how humans think when they are faced with an impossible situation.

Data sharing is another important aspect of one's right to privacy. When we come to the point in the algorithmic policing landscape where individuals' data needs to be shared between different law enforcement agencies across provinces and perhaps with the private sector, the laws

are rather harsh for the policing institutions (Robertson et al. 84). According to R v Orlandis-Habsburgo, 2017 ONCA 649 at paras 31-33 and 98-115; R v Cole, 2012 SCC 53; R v Reeves, 2018 SCC 56; R v Spencer, [2014] 2 SCR 212, law enforcement agencies cannot accumulate personal data from private institutions that is not readily available from other sources (Robertson et al. 84). And if these agencies tried to obtain this data, it would be an unlawful evasion of privacy and would break laws that were established to protect and safeguard the citizens of Canada from potential abuse of power (Robertson et al. 84). Expanding on this further, what it simply means is that if policing agencies were allowed to obtain data through the private sector that they could not obtain through constitutional means, it would give the government an unfair advantage in the form of the ability to observe individuals without necessary oversight (Robertson et al. 84). This level of surveillance can be extremely alarming for both the administration and the people if it is not properly supervised. It ties back to the principles of trust that needs to exist between a government and its subjects. And this unauthorized surveillance will definitely not play well in building trust, as people will clearly see their right to privacy being jeopardized.

The Supreme Court's model of informational privacy rights was enhanced in R v TELUS (Singh 8). In this case, the police requested that TELUS provide access to texts for two suspects (Singh 8). The police did not just request access to historical data; they also asked TELUS to be able to view every single text message that either of the suspects sent in the near future (Singh 8). The presiding judge considered this request to be along the same lines as requesting a wiretap for communications that had not yet taken place (Singh 8). This was the point in Canadian history where it became unlawful for the police to simply request prospective information from private companies without prior authorization similar to a warrant (Singh 8). This case is

particularly important while trying to distinguish what data an algorithmic policing model can and cannot use, even if the data exists. There needs to be regulatory teams at police stations that routinely check that the AI is making decisions based on data sets obtained legally and ethically.

The last principle that we will look review in this paper is the principle of data accuracy. The ICCPR allows individuals to request to have their personal information updated that is being used in the private or public sectors (Robertson et al. 84). Inaccurate data can have unforeseen consequences for the public as well as the government. Errors in the data will lead to inaccurate predictions by the AI models and can affect the overall reliability of the model. In this case, the AI model could be built with the best intentions and with the proper precautions, but it could still give out faulty results due to biased data, which is much harder to track down. Interestingly, the Canadian Police Information Center database, which stores all criminals' historical data and is often used by law enforcement agencies, has been critiqued for being irrelevant and imprecise (Robertson et al. 85). The Ontario Court of Justice has asserted that it is the government's responsibility to update the information in their databases as it is used to make decisions on the subject of a person's liberty (Robertson et al. 85). Using inaccurate information to build models that lead to wrongful search and seizure can really dampen the trust between a government and the public and chip away at the rights of a person.

In this paper, we provide an in-depth analysis of algorithmic policing, which is basically an intelligent computer system making the same decisions as human police officers. We saw that, despite being an incredible concept, it is a long way from being fully immersed into society. We assessed the idea of algorithmic policing from the angle of ethics, i.e., the role the ethical principle of trust plays in making a society trust these AI systems and, in turn, trust their governments. Our next objective was to review algorithmic policing in line with the laws set

forth in the Charter of Rights and Freedoms, with a focus on the right to privacy. We reviewed specific examples of real-life cases to see how a person's privacy can be impacted by AI models if extreme precaution is not taken in building these models.

All in all, we believe that this paper is a decent starting point for a much larger topic that cannot be contained within the constraints of this paper. That said, if we were to boil down the motives of this paper to one sentence and end with a final message, it would be this: If you are planning to work as a software engineer, performing advanced data analytics, and building AI models and taking charge of the foreseeable future, remember to always re-think your ideas to ascertain if there are any *ethical and legal issues in analytics and AI*.

Works Cited

Government of Canada, Department of Justice. Learn about the Charter- Canada's System of Justice. 12 Apr. 2018, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/learn-apprend.html.

Kenyon, Miles. Algorithmic Policing in Canada Explained. Citizen Lab, University of Toronto, 1 Sept. 2020, https://citizenlab.ca/2020/09/algorithmic-policing-in-canada-explained/.

Chatila, Raja, et al. "Trustworthy AI." Reflections on Artificial Intelligence for Humanity, Springer International Publishing, 2021, pp. 13–39, https://doi.org/10.1007/978-3-030-69128-8_2.

Omrani, Nessrine, et al. "To Trust or Not to Trust? An Assessment of Trust in AI-Based Systems: Concerns, Ethics and Contexts." Technological Forecasting & Social Change, vol. 181, 2022, p. 121763–, https://doi.org/10.1016/j.techfore.2022.121763.

Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto.

Singh, Shawn. "Algorithmic Policing Technologies in Canada." Manitoba Law Journal (1966), vol. 44, no. 6, 2021, pp. 246–88.

Hobson, Zoë, et al. "Artificial Fairness? Trust in Algorithmic Police Decision-Making." Journal of Experimental Criminology, 2021, pp. 1–25, https://doi.org/10.1007/s11292-021-09484-9.