Who Watches the Watchers: Oversight of State Surveillance

MARK PACKULAK*

ABSTRACT

Surveillance capability is rapidly advancing. What is being captured is more than just stock footage. Powerful artificial intelligence software that uses facial recognition technology can track details about people and their behaviour patterns. This technology is being used to crack down on people in authoritarian states and to extensively monitor citizens in many democratic states. So far, the regulation over how this technology is to be used has largely been absent, leading to tremendous violations of privacy rights in some cases.

The use of this type of technology by the state, specifically the police, could constitute an unconstitutional breach of the reasonable expectation of privacy. Canadian courts have so far held that individuals do not enjoy a right to privacy in any public places. What rights should an individual have over their face and the collection of their information by the state?

This paper first examines the collection of biometric identification data as compared to previous biometric identification collection and use. Secondly, this paper examines some of the capabilities and pitfalls of state surveillance. Finally, this paper suggests that as dangerous as state surveillance can be, it should be a staple of effective policing, if there is sufficient oversight.

The police should have access to the most modern and efficient technology available to serve the public effectively. However, the dangers of

* Mark Packulak is a proud graduate of the University of Manitoba with a Batchelor of Arts and a Juris Doctor degree. He is currently articling with Riverwood Community Law Centre, an office of Legal Aid Manitoba. He is married to Chantal and they have four children, Katherine, Isabelle, Sophie, and Mark. He was awarded the Class of 1980 award for the Class of 2022 and he hopes to make a contribution to criminal law in Manitoba.

a complete dissolution of privacy necessitate oversight for the police. There must be an independent body to collect and utilize this technology that the police may access through a judicially operated warrant-like system. Effective policing and privacy can coexist and serve the public good.

Keywords: Surveillance; Facial Recognition; Artificial Intelligence; Reasonable Expectation of Privacy; Video; Warrant; Oversight.

I. INTRODUCTION

Observation is a central part of the Canadian justice system. Many cases have turned on the strength of witness' observation evidence. Public actions carry the well-understood possibility of observation. The State is free to observe everything that happens in the public sphere. Historically this has been the function of police officers on patrol, but technology is expanding the observation powers of the state in a largely unregulated fashion. The protections found in the *Canadian Charter of Rights and Freedoms* (the "*Charter*")[1] cannot be solely managed by the courts through an ends and means analysis.

Police departments have used and continue to use technology without sufficient public oversight. Surveillance cameras have been used for many years to observe and protect from criminal activity. Recent advancements in camera and Artificial Intelligence ("AI") technology are being used by police without the crucial step of public debate. Biometric identification and AI algorithms which can predict criminal behavior are blurring the lines between effective policing and a police state.

Thus far the Supreme Court of Canada ("SCC") has held in *R. v. Tessling* that "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public."[2] This suggests that the act of leaving any place where someone enjoys a reasonable expectation of privacy is implied consent to be observed. The *Charter* protects from unreasonable search or seizure by the state. The courts face a tough challenge to protect *Charter* rights in an era when technology is rapidly evolving. The *Charter* is a living tree and is intended to grow with society and technology. Parliament and the courts must ensure that the principles of the *Charter* grow with

---

1 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 91(24).

2 *R v Tessling*, 2004 SCC 67 at para 40 [Tessling].

technology. The SCC echoed this principle in quoting professor Paul Freund when he admonished American courts "not to read the provisions of the Constitution like a last will and testament lest it become one."[3]

Today politicians and courts are facing tremendous pressure to reform policing. Restricting technological improvements discussed in this paper is not the same thing as reforming policing. Making policing less effective and more onerous does not address systemic issues in our system. The police must utilize surveillance technology that can assist in swift and accurate law enforcement, but because this technology is so dangerous, it must be regulated through an independent agency and accessed through a warrant procedure. This paper will first examine the existing law of reasonable expectation of privacy of personal information, then examine the evolving surveillance technology, and finally suggest a scheme that should be adopted regarding its use.

II. Biometric Incrimination

This paper primarily examines the need for oversight of state use of video surveillance, however given that video surveillance captures personal information it is useful to examine the adoption of other types of personal information collection authorized by law. In 1944, Chief Justice Robson of the Manitoba King's Bench stated that "the taking of these prints was like the taking of statements without warning, and the result could not be used against the defendant."[4] In the above case, fingerprints required for a job application at a World War II defence industries plant were matched to an outstanding warrant from Detroit, Michigan. Long before the crafting of the *Charter*, Chief Justice Robson equated the seriousness of the collection of personal information to that of a right to silence. Unless authorized by statute, the intention of the collection of biometric information must be disclosed and used only for that purpose. A brief exploration of the history of personal biometric information will inform further arguments on the need to safeguard personal information from state surveillance.

A. Fingerprints

---

3 *Hunter et al v Southam Inc*, [1984] 2 SCR 145 at 155, 11 DLR (4th) 641 [Southam].

4 *Danilhik (Re)*, [1944] CanLII 440 (MB QB), at 267 82 CCC 264 [Danilhik].

Fingerprints have been a staple of law enforcement for over one hundred years. Many forms of biometric identification had been experimented with before fingerprints became the common standard for personal identification. Like all technology and procedures used for law enforcement, fingerprinting had to be accepted and directed for use. In 1934, Chief Justice Thompson of the Supreme Court of British Columbia had difficulty accepting fingerprint evidence as expert evidence and instead included the evidence as opinion evidence. He referenced the 1927 version of the *Identification of Criminals Act*[5] which required any person in lawful custody to be subjected to "the Bertillon Signaletic System, or to any measurements, processes or operations sanctioned by the Governor in Council having the like object in view."[6]

Systems such as the Bertillon Signaletic System relied upon a series of 11 measurements of fixed points on the body. Cards were kept with the data on them. The system is said to have produced identical identification of two African American men in the Leavenworth Kansas Penitentiary, but their fingerprints were distinct. Although this story, as Simon Cole writes, is almost certainly anecdotal, it does represent the process that many U.S. states went through to attain more accurate forms of identification.[7]

Although fingerprinting was not new in 1934, it had not become a sufficiently accepted science for Chief Justice Thompson to admit as anything but opinion evidence.[8] Of course the current version of the *Identification of Criminals Act* ("*ID Act*") allows for the fingerprinting and photographing of anyone charged or convicted with an indictable or hybrid offence.[9] The admission of DNA evidence faced a similar battle for admission, but with the aid of more precedent.

B. DNA

John J. Walsh, Q.C. wrote about prosecuting *R. v. Allan Joseph Legere* in 1991 and the decision to adduce DNA evidence. The trial featured an extensive *voir dire* hearing regarding the admissibility of DNA evidence that

---

5 *Identification of Criminals Act*, RSC 1927, ch 38.

6 *R v De'Georgio*, [1934] CanLII 417 (BC SC) at 378-379, [1934] 3 WWR 374 [De'Georgio].

7 Simon Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification*, (Cambridge: Harvard University Press, 2002) at 140-144.

8 *De'Georgio*, *supra* note 6at 380.

9 *Identification of Criminals Act*, RSC 1985, c I-1, s 2(1).

lasted for 24 days over the course of three months.[10] The Crown called three well-credentialled experts and the defence called a well-credentialled DNA skeptic. Although both sides conceded that every individual has unique DNA, there was considerable argument over the determination of match probability between samples and the accused. At one point the defence expert drew sharp public criticism over the assertion that a high level of inbreeding in New Brunswick was likely to give false match probability results.[11]

Although not the first case in Canada to admit DNA evidence, *R. v. Legere* was a seminal case for the admission of DNA in Canada. This was in part due to the thorough decision of the trial judge which was upheld by the New Brunswick Court of Appeal and denied being heard by the SCC.[12] DNA, like fingerprinting before it, became the new evidentiary standard.

C. Compelling Biometrics

The need for reliable methods of identification is important for many layers of society, but especially so in criminal law. DNA evidence has been used to exonerate as well as to incriminate. According to the Innocence Project, 375 people in America have been exonerated by DNA, 21 of which served time on death row.[13] DNA is a powerful investigative tool, especially with national and international DNA databanks. Compelling and retaining DNA in Canada is regulated by statute, without which, state collection would cast too wide a net. In *Hunter v. Southam*, the SCC examined the *Charter* compliance of legislated search powers. Authorized searches must be conducted based on investigation rather than suspicion: "the state's interest in detecting and preventing crime begins to prevail over the

---

10 "Allan Legere Digital Archive: Voir Dire – Transcript" (last visited 13 April 2022), online: University of New Brunswick Allan Legere Digital Archive <www.unb.ca/fredericton/law/library/legal-materials/digital-collections/allan-legere/voirdire-transcript.html> [perma.cc/AQ6N-6MGQ].

11 John Walsh, "R v. Allan Joseph Legere and DNA Evidence: Reminiscences" (last visited 13 April 2022) at 9, online (pdf): University of New Brunswick: Allan Legere Digital Archive <www.unb.ca/fredericton/law/library/_resources/pdf/legal-materials/allan-legere/comms_bibliography/legere_trial_digital_collection__r__v__allan_joseph_legere_.pdf> [perma.cc/9L3V-CJRG].

12 *R v Legere*, [1994] CanLII 3851 (NB CA), 156 NBR (2d) 321 [Legere].

13 "Exonerate the Innocent" (last visited 27 June 2022), online: *Innocence Project* <innocenceproject.org/exonerate/#:~:text=To%20date%2C%20375%20people%20in,prison%20before%20exoneration%20and%20release.> [perma.cc/9S5S-5642].

individual's interest in being left alone at the point where credibly-based probability replaces suspicion."[14]

In America, police used commercial DNA services as a databank to solve cold cases. Their aims, while laudable, clearly infringed on the rights of those who submitted their DNA for another purpose. Companies bowing to public pressure began to refuse police access to their databanks.[15] This example demonstrates the need for regulated protection against unintended self incrimination.

The warrant process is the best regulation available for the collection of biometric information. For a police officer to obtain a warrant to compel identification evidence they must comply with the scheme in section 487.05 and 487.092 of the *Criminal Code* of Canada.[16] An officer must demonstrate that there are reasonable grounds to believe that there is bodily substance evidence and that the person who is the subject of the warrant was a party to the offence. Identification evidence has a tremendous impact on the accused. The process of obtaining a warrant is an important check on the power of the state to compel.

Section 2 of the *ID Act* allows for the collection of fingerprints and photographs of anyone charged with an indictable offence. In *R. v. Beare; R. v. Higgins*, both accused were charged with criminal offences and served with a summons to be fingerprinted prior to their trial. The suspects refused to attend and challenged the constitutionality of section 2 of the *ID Act*. Justice La Forest in writing for the majority found that the constitutional rights of the accused were not infringed since the process for obtaining a summons requires the police to demonstrate reasonable and probable grounds.

D. Retaining Biometrics

Police in Canada retain all fingerprints at the Canadian Police Information Centre in Ottawa. The information stored here is shared with law enforcement outside of Canada as well. The collection of fingerprints and photographs "provide a lasting record and may tie an individual to

---

14 *Southam*, *supra* note 3at 167.

15 See Jon Schuppe "Police were cracking cold cases with a DNA website. Then the fine print changed" (23 October 2019), online: NBC News <www.nbcnews.com/news/us-news/police-were-cracking-cold-cases-dna-website-then-fine-print-n1070901> [perma.cc/VW75-TBKW].

16 *Criminal Code*, RSC 1985, c C-46, s 487.

other crimes."[17] The collection of fingerprints and photos taken upon arrest or warrant is authorized by statute, but the storage for future use treads close to the right against self-incrimination. The Court in *R. v. Dore* examined the use of fingerprints that were voluntarily surrendered for exclusion from charges that were subsequently dropped when the fingerprints did not match a sample from a crime scene.[18] The fingerprints were retained and later compared against another crime scene which did match the appellant.

The Court found that once the fingerprints either did not match, or where an accused is acquitted or receives a stay, the accused may request to have the records of their prints destroyed. If an accused requests this, then they have asserted their right to privacy over their own identification information and the state must comply. However, if the accused is convicted then the state may retain the fingerprints or photographs in accordance with the *ID Act*. The *ID Act* stops short of protecting individuals from future incrimination by failing to require the state to destroy records after their unsuccessful testing, though the ability to have biometric information destroyed recognizes that individuals should enjoy a basic right to privacy. The Court recognized this principle when they upheld the overturning of a conviction in *R. v. Borden*. An accused provided DNA for the purpose of exoneration in one investigation, but the police used the sample to charge them in another investigation.[19]

Unfortunately in society, the expansion of surveillance techniques has often been exposed rather than debated. Leaks by Julian Assange, Chelsea Manning, Edward Snowden, and many others who risk prosecution to expose undebated use of technology, demonstrate that too often a state that operates like a child who would rather ask for forgiveness than permission when it comes to observing their citizens.

III. Reasonable Expectation of Privacy

The SCC has repeatedly held that there is a low expectation of privacy in the public sphere.[20] A police officer is well within their duty to observe

---

17 Robert Solomon et al, "The Case for Comprehensive Random Breath Test Programs in Canada: Reviewing the Evidence and Challenges" (2011) 49:1 Alta L Rev 37 at 64

18 *R v Dore*, 2002 ONCA 2845, 54 WCB (2d) 691 [Dore].

19 *R v Borden*, [1994] 3 SCR 145, 119 DLR (4th) 74 [Borden].

20 See *R v Boersma*, [1994] 2 SCR 488, 31 CR (4th) 386; *R v Stillman*, [1997] 1 SCR 607 at 611, 144 DLR (4th) 193; *R v Evans*, [1996] 1 SCR 8 at 33-34, 131 DLR (4th) 654; *R v*

and even surveil anyone in a public space. If Canada applies this principle to video surveillance, then cheaper and more effective surveillance technology could observe a majority of Canadian society. The SCC contemplated the careful balancing act needed between individual privacy rights and state interests in *Hunter v Southam*:

> [W]hether it is expressed negatively as freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.[21]

AI facial recognition, predictive algorithms, and uninformed capture of personal data constitute a huge risk to the privacy expectations of the public.

A. Public Space

As early as 1862 statutes prohibiting wiretapping were enacted in California. A man by the name of D. C. Williams was convicted under statute of listening to corporate communication to sell to stockbrokers.[22] Even with the invention of video surveillance, the practical effect was monitoring or review by a human agent.

A human agent watching a live or recorded video feed is not very different to a security guard on patrol. Cameras in plain sight certainly provide some warning to the public of observation. This level of surveillance is tolerable, often for the protection of property, but what would most people think of a digital surveillance network which captured their every move in public? Consider the indignation of Justice La Forest in his dissent of *R. v. Wise* (1992) which only involved the use of a beeper to allow police to track the movement of a suspect's car:

> I must confess to finding it absolutely outrageous that in a free society the police or other agents of the state should have it within their power, at their sole discretion and on the basis of mere suspicion, to attach a beeper on a person's car

---

Wong, [1990] 3 SCR 36, 60 CCC (3d) 460; *R v Mills*, 2019 SCC 22; *R v Tessling*, 2004 SCC 67; *R v Wise*, [1992] 1 SCR 527, 70 CCC (3d) 193 [Wise].

21 *Southam*, *supra* note 3at 159-160.

22 See Precise Digital, "A Brief History of Surveillance in America" (28 March 2018), online: *Precise Digital* <www.precisedigital.com/a-brief-history-of-surveillance-in-america/> [perma.cc/46GB-78NP].

> that permits them to follow his or her movements night and day for extended periods.[23]

Surveillance must be considered not only in the context of the current capability, but also in the reasonable assumption that capability will only improve and cost will decrease.

B. Police Surveillance

The public sphere carries a generally low expectation of privacy. A police officer on patrol is generally accepted to be able to observe any actions in public. A police officer can only be in one place at one time to observe the public. Actively monitored video surveillance can increase the effectiveness of every individual officer. Think about a camera mounted on every corner in every direction that would monitor a sizable grid. If a crime were observed, the officer patrolling the grid could be directed to the scene or suspect by a camera observer.

This system would still have significant gaps since the controller could only watch one screen at a time and would only be able to observe actions. They may recognize a dangerous individual but would only be able to do so if they could recognize them through the camera at a distance. Facial recognition programs can rapidly examine all the faces on the screen and match them to databases. Now instead of a room with dozens of monitors statically focused on a street, there are hundreds of feeds running through a program which stores each face, location, time, direction of travel, and activity of each person walking that street.

In the city of Chongqing in China, 2.58 million cameras monitor 15.35 million people, and facial recognition software alerts police to the presence of people in a crowd who match a person of interest.[24] It is easier to imagine such a system in an authoritarian country where human rights violations are common and expectation of privacy is not a right, but the city of London ranks 3rd in Comparitech's 2021 list of most surveilled cities.[25]

---

23 *Wise*, *supra* note 20.

24 See Matthew Keegan, "Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled" (2 December 2019), online: *The Guardian* <www.theguardian.com> [perma.cc/3E5N-Z7V2].

25 See Paul Bischoff, "Surveillance camera statistics: which cities have the most CCTV cameras?" (17 May 2021), online: *comparitech* <www.comparitech.com> [perma.cc/298N-HJNN].

Technological advances are required for this level of surveillance, but so is the consent of the public. The dramatic increase in public paranoia over crime that occupied many people in the 1990s evolved into fear of terrorism post 9/11. The moment that the consciousness of the world realized that the Twin Towers could be destroyed by a small group of fanatics cemented security as a concern in every free nation.

C. Facial Recognition

Facial recognition programs can be tremendously beneficial. Think of picture accumulation in the modern era. Many people have photo albums of their childhood with occasional pictures printed from special family events. Physical film limited the taking of photos due to cost and time to print. Digital photos resulted in generations now that accumulate thousands of photos each year. Why settle for one perfect shot when you can take twenty and touch up the best one?

Programs were developed to sort photos and eliminated duplicates from overfilled drives. This same technology has been taught by developers to better recognize the subtle differences in faces. Technology to help can be easily turned to more nefarious purposes. Think about cloud storage such as Apple's iPhoto, Facebook, or Google Drive which save millions of images each month. It is convenient for users to be able to sort photos by different family members and friends, but who is being captured in the backgrounds of these photos? It is ludicrous to suggest that individuals obtain the permission of everyone in a public square before they take a picture, and certainly case law suggests that a public space carries a low expectation of privacy.

Facebook settled a lawsuit on January 30, 2020 for $550 million because it used facial recognition technology to create digital profiles of everyone in uploaded photos. Other tech companies are facing similar legal challenges to their nearly unregulated use of facial recognition software to compromise the privacy of users and non-users alike.[26]

The ability of mass state surveillance powered by AI technology to capture information from wide sections of public life constitutes an infringement of privacy. Actions performed in public are often intended for a specific recipient, rather than for observation and profiling by an advanced public surveillance system. Consider what the SCC said in *R. v. Dyment*

---

[26] See Samuel D. Hodge Jr., "Big Brother Is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century" (2020) 89:1 U Cin L Rev 30 at 79.

regarding the voluntary surrender of a blood sample by a doctor to a police officer:

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.[27]

There is a weakness in the privacy protection by the courts when it comes to video surveillance. Most of the cases that come before the courts deal with specific infringements of privacy and are not always applicable to the technology used to infringe the privacy. The other issue is that trial and appeal processes take an extraordinary amount of time to resolve. There is no prohibition on the market from using the impugned technology while a case is heard and appealed. Even if surveillance technology is found to infringe privacy rights, successive generations of the same technology may render it substantively different than the impugned technology. It falls to the government to enact legislation that protects the rights of individuals to their privacy. This too though, often falls dreadfully behind the curve of technological improvement.

Consider the case of *Alberta v. Hutterian Brethren*. For years the colony had obtained a photo exemption from their drivers license because of a religious belief restricting the creation of any members' image. This case took more than three years to work its way to the SCC, and the Court found that the infringement of their religious rights was justified by the purpose of the legislation under section 1 of the *Charter*. This case was decided on the basis of religious belief, but privacy was a central untouched theme of the arguments. Justice Abella, writing for the dissent, emphasized the intensely private nature of the colony. She outlined that their lifestyle and interest in privacy extents to their every interaction with the state, and that the infringement of their religion was not just a violation of their religious beliefs, but of their privacy as well.[28]

Facial recognition technology during the time that this case was heard was only emerging into practical use. The government of Alberta wanted to begin using facial recognition with their drivers licensing database to prevent fraud. This suggests that the process had already started or was being

---

27 *R v Dyment*, [1988] 2 SCR 417 at 429-30, 55 DLR (4th) 503 [Dyment].

28 *Alberta v Hutterian Brethren of Wilson Colony*, 2009 SCC 27 at para 166 [Hutterian].

implemented without public consent or discussion. Privacy was a secondary concern to religious freedom in this case, but what would the reaction be of colony members if it was understood that all across the province of Alberta, the photos that they were now legally required to submit would be accessible to scanners and cameras everywhere?

D. Programming Facial Recognition into AI

To better understand the impact of unconsented capture of a digital likeness of someone's face it is useful to examine the process of capturing and individual likeness. The B.C. Office of the Privacy Commissioner investigated the use of facial recognition by the Insurance Corporation of B.C. Their report is useful to understand the general process of capturing a likeness for facial recognition. According to the report, this happens in three stages:

1. Enrollment. A digital image such as a driver's licence photo is analyzed. Software measures the image line by line and makes grades of skin colour and texture. The image is converted into binary code based on these and other factors.

2. Storage. The unique binary code for each image is stored in a database for future comparison.

3. Matching. This process involves the greatest influence of human bias. Unique binary codes for each image are compared to new images received by the system each day. Images are evaluated for similarities with other existing binary image codes. When similar photos are found, a report is generated for the system which must be reviewed by a panel to examine whether the likeness is in fact the same person. In this way the existing bias of the examiners is training the system.[29]

The photos to digitize for this and other agencies both public and private can come from a variety of sources, but an important distinction regarding privacy is whether the photo was captured with or without the subject's knowledge. In 2021, the Office of the Privacy Commissioner of Canada released a report of an investigation into Clearview AI, Inc.[30]

---

[29] Elizabeth Denham, *Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia*, Office of the Information and Privacy Commissioner for British Columbia, Report F12-01 (BC: Information & Privacy Commissioner, 2012).

[30] Canada, 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

Clearview is an American company that provides a paid identification and profiling service to law enforcement agencies. Clearview's AI technology data mines millions of images from social media sites and other pictures publicly uploaded by users to build profiles. Law enforcement agencies can request identification with only a photo of a suspect.

The Office of the Privacy Commissioner of Canada found that Clearview violated Canada's privacy laws, but the resolution was only a voluntary suspension of services offered to Canadian law enforcement agencies for a period of two years to seek guidance. This does not prevent Clearview from operation or continued data mining to identify Canadians or build profiles on them. Such an AI system plugged into real time surveillance could direct real time police operations. Police in cities such as Los Angeles and Chicago have employed AI based predictive policing. This technology uses statistics, surveillance, and algorithms to feed AI which directs policing to areas of concern.[31]

The known weakness of AI is the same as those who program it. Programs are taught what to look for and what indicators are to be used by programmers or users. For the programmers, it is nearly impossible to avoid programming bias into the system. Predictive policing for example often utilizes statistics. Over policing and disproportionate policing of racialized minorities feed data into predictive AI which responds with greater policing. This creates a cycle of greater policing and overrepresentation. Aaron Shapiro argues that the faults inherent to AI predictive policing lie in the society using it rather than the method of policing.[32]

E. Capture without Consent

Consenting to have a digital scan taken of a face carries the consent to have that scan analyzed by the agency doing the collection. A more concerning capture is one which does not come with consent. In the United States, the American Civil Liberties Union is currently engaged in a freedom of information lawsuit against multiple federal agencies for data

---

Privacy Commissioner of Alberta, (Ottawa: Office of the Privacy Commissioner of Canada, 2021)

31 See Tim Lau, "Predictive Policing Explained" (1 April 2020), online: *Brennan Center for Justice* <www.brennancenter.org/our-work/research-reports/predictive-policing-explained> [perma.cc/UB5M-TWH6].

32 Aaron Shapiro, "Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing" (2019) 17:3/4 Surveillance & Society 456 at 469.

on their crowd surveillance programs.[33] During many of the protests against officer shootings in recent years, many states have surveilled crowds. In some cases drones are used from high altitudes to disguise their presence. In other cases police forces operate hundreds of drones to record vast amounts of footage. In every case these drones do not just capture random individual's actions, but are able to take high resolution images of individuals for identification.[34]

Beyond crowd control, many cities around the world employ public surveillance cameras to record and identify individuals. The Canadian jurisprudence has yet to distinguish mass public surveillance by the state with a public expectation of privacy. Current cost and technological restrictions bearing on continuous surveillance of all public spaces cannot always be assumed to limit surveillance. It is a mistake of jurists to conclude that because current technology may still allow for some privacy from state observation in public spaces, that it is only minimally impairing to *Charter* rights of unreasonable search.

R. v. Voong is such a case where a specific instance of facial recognition technology fails to consider the larger consequences of allowing such a search. The applicant in this case was found to be holding multiple driver's licenses, some with unpaid fines and court summons. The search was conducted using facial recognition software scanning the database of driver's licenses. The Court agreed with the Crown: that there is no expectation of privacy in a photograph or information submitted to obtain a drivers license.[35]

It is not hard to argue that photos submitted to the Ministry of Transportation for driver's licenses could be subjected to scrutiny to prevent fraud.[36] Justice Libman concluded that since the information contained in a search of a driver's license database is similar to information commonly required for many other services, there can be no expectation of privacy even over the photos. The glaring difference is that those other agencies do

---

33 *American Civil Liberties Union et al v United States Customs and Border Protection et al*, Dist Ct NY 1:21-cv-10430-ER.

34 See ACLU, "ACLU v CBP-FOIA Case for Records Relating to Government's Aerial Surveillance of Protestors" (last modified 7 December 2021), online: *ACLU* <www.aclu.org> [perma.cc/762A-686S].

35 *R v Voong*, 2018 ONCJ 352 [Voong].

36 See *The Manitoba Drivers and Vehicles Act*, CCSM C-D104, s149.1(4) was amended in 2008 to allow the use of facial recognition technology. It also allows the possibility of future technology to be used for the purpose of identification.

not have the right to deny liberty or impose other harsh penalties. The state requires everyone that wishes to drive on public roads to be licensed. The Court already ruled that photos can be compelled on driver's licenses and as such the submission of a photo is compulsory. While it is true that a driver's license applicant should reasonably conclude that their information and photo is accessible to the police for the determination of driving legally and tracking driving offences, it is not reasonable to conclude that supplied information and photo would be used for any other purpose by any other function of government. Justice Libman did not conclude that such other searches would be legal, but in stating that the applicant had no expectation of privacy over their information, combined with no specific caution or exclusion over other uses, it is possible to conclude that driver's license information is the property of the state for any purpose they see fit.[37]

F. Reasonable Expectation of Privacy in Public Spaces

The SCC dealt with this concept of privacy in public spaces in a more recent case *R. v. Jarvis*.[38] In this case, a teacher in a public high school was using pen camera technology to record students. All the recordings were in public spaces which the accused was allowed to observe students. The trial judge and the Court of Appeal followed precedent and found that students could not have a reasonable expectation of privacy in public spaces. The Courts had no difficulty finding that the offender made the recordings for a sexual purpose since he filmed girls' chests, but they could not find a reasonable expectation of privacy.

The SCC found that "simply because a person is in circumstances where she does not expect complete privacy does not mean that she waives all reasonable expectations of privacy."[39] The Court examined the difference in observing and recording, noting that recording makes available so much more than a human eye in passing can observe. A crucial point in this judgment is the distinction the Court draws between school security cameras and the intimate recording by Mr. Jarvis. The Court indicates that the presence of security cameras connotes a general understanding of being observed and that students can still hold an expectation of how they are

---

37 *Voong*, *supra* note 35 at paras 46-47.

38 *R v Jarvis*, 2019 SCC 10 at para 61 [Jarvis].

39 *Ibid* at para 37.

being observed whereas Mr. Jarvis did not obtain this same understood consent.

The Court went further and stated that "individuals going about their day-to-day activities — whether attending school, going to work, taking public transit, or engaging in leisure pursuits — also reasonably expect not to be the subject of targeted recording focused on their intimate body parts (whether clothed or unclothed) without their consent."[40] Modern surveillance abilities capture much more than that. Imagine where you travel, how often, with whom, what you purchase, what you view, who your eyes linger on, what you eat, and much more all being recorded and cataloged. That information is matched to public records to track and analyze the details of your life to predict criminal behaviour which could result in an officer knocking on your door for a friendly conversation about disturbing trends in your habits. It is a relief that the SCC found that Mr. Jarvis violated students' reasonable expectation of privacy.

G. Reasonable Expectation Test

When evaluating whether there exists a reasonable expectation of privacy the SCC uses a totality of the circumstances test from *R. v. Edwards*:

1. A claim for relief under s. 24(2) can only be made by the person whose *Charter* rights have been infringed.
2. Like all *Charter* rights, s. 8 is a personal right. It protects people and not places.
3. The right to challenge the legality of a search depends upon the accused establishing that his personal rights to privacy have been violated.
4. As a general rule, two distinct inquiries must be made in relation to s. 8. First, has the accused a reasonable expectation of privacy. Second, if he has such an expectation, was the search by the police conducted reasonably.
5. A reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances.
6. The factors to be considered in assessing the totality of the circumstances may include, but are not restricted to, the following:
    a. presence at the time of the search;
    b. possession or control of the property or place searched;
    c. ownership of the property or place;

---

40 *Ibid* at para 90.

d. historical use of the property or item;

e. the ability to regulate access, including the right to admit or exclude others from the place;

f. the existence of a subjective expectation of privacy; and

g. the objective reasonableness of the expectation.[41]

As stated in *R. v. Cole*, a totality of circumstances test is "one of substance, not of form," which means that every case is contextual to the circumstances.[42] During the oral submissions of *R. v. Jarvis*, Justice Moldaver probed counsel on the totality of circumstances test. He stated that a student may possess a reasonable expectation of privacy in a public space, but that the recording by a teacher in a position of trust may violate that in ways that a contemporary may not.[43] He later referenced observation in a locker room where an expectation of privacy is unreasonable between those changing but is reasonable with regard to recorded or sexualized viewing of those changing.[44] The Canadian Civil Liberties Association's submissions characterized the reasonable expectation of privacy in a public setting to be conduct or purpose-based over location-based.[45]

The Court in *R. v. Jarvis* had to deal directly with the issue of whether an individual can assert a reasonable expectation of privacy in a public setting. The Court clearly sided with the Crown that the students were exploited and that they enjoyed a reasonable expectation of privacy in situations where the location held no connotation of privacy. The totality of circumstances test elevated otherwise harmless viewing into criminal behaviour. Applying the judgment in *R. v. Jarvis* to state surveillance would ask the question of whether state surveillance in public spaces, however intrusive, is a circumstance that violates a reasonable expectation of privacy. The final section of this paper proposes that the state should have at its disposal every technology to surveil for the purposes of law enforcement, but that to balance privacy concerns, it should be required to follow a warrant process to access the surveillance.

---

41 *R v Edwards*, [1996] 1 SCR 128 at 145-46, 132 DLR (4th) 31 [Edwards].

42 *R v Cole*, 2012 SCC 53 at para 40 [Cole].

43 *R v Jarvis*, 2019 SCC 10 (Oral argument Appellant) at 18m:45s.

44 *Ibid* (Oral argument Respondent) at 01h:13m:16s.

45 *Ibid* (Oral argument Intervenor) at 39m:10s.

IV. PRIVACY PROTECTION

Twice in SCC judgments, Justice La Forest references the novel *1984* by George Orwell when writing about police surveillance.[46] In *R. v. Wong* he writes that "we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy."[47] The invocation of dystopian fiction in reference to SCC cases should not be discarded as mere hyperbole. Justice La Forest considered surveillance techniques employed by Canadian police to be a serious threat to privacy. These cases were heard in 1990 and 1992, before the invention of modern surveillance methods which would rival the imagination of George Orwell.

A. Justified Infringement

The SCC in *Hunter v. Southam* stated that protection of an unreasonable search also provides a reasonable expectation of privacy. If technological ability is the limit to the state observing all members of society, then we should reasonably expect that the technological barriers preventing constant surveillance will only decrease. Society must then develop rules for observation by the state under current constraints that will port to a system with more advanced technology. However, as stated by Paul Bischoff, "unfortunately, there is a paucity of laws on the use of surveillance cameras in public places, and only a small number of jurisdictions have enacted legislation to regulate these activities."[48]

The lack of oversight is particularly concerning given some of the technological capabilities already available in drone technology. Traditional surveillance rules cannot compete with the plethora of relatively low-cost surveillance abilities of drone technology. Durakovic & Durakovic elaborate:

> It is the convenience of drones to be equipped with different and numerous sensors that enables them to track changes from a distance through the visible spectrum, electromagnetic spectrum, biological and chemical changes, with the ability to automatically detect target objects, to track positions through GPS

---

46 *Wise supra* 20 at 41; *R v Wong*, [1990] 3 SCR 36 at 47, 60 CCC (3d) 460 [Wong].

47 *Wong*, *supra* note 46.

48 Bischoff, *supra* note 25at 33.

> systems, to register changes in real-time high-resolution cameras, giving huge potential for police use.[49]

Protection of civil liberties through precedent is by its very nature behind the technological curve. Police services in Canada are managed through civilian oversight, but to respect privacy and self-incrimination rights, public disclosure of operational practices must be implemented.

The fact that technology will allow for a more invasive state does not mean that it cannot also realize the vision of a safer society. Public institutions, including the police, owe a debt to society to be as efficient and thorough in their service to society as they can be. Technology that can improve the speed and accuracy of investigations should be implemented. However, the most important part about using improved surveillance will be oversight. All data and surveillance should run through an agency independent of the state or police. All available information, useful to police in their pursuit of a safer society should be available with a warrant-type process. Meeting a similar standard, as determined by the judiciary, would prevent even the question of abuse while serving the interests of justice. The current lack of oversight does more harm to the public perception of police and state power to protect citizens.

B. Oversight

The state is an entity of the public. In a free and democratic society, elections populate government positions with people who are meant to represent the public at large. What activities are criminalized or incentivized are meant to represent the values of the public as a whole. Certainly laws are meant to guard against a tyranny of the majority, but many of these laws require someone withstanding to challenge them. Law enforcement are members of the public and are tasked with protection of the public good. Surveillance by law enforcement has expanded in a large part through the social need for security in a post 9/11 world.

Crime and terrorism prevention are a laudable goal, but there is a cost to a society that surrenders their freedoms and privacy for feelings of security. The fundamental idea of property is a right to privacy and exclusion from that property. American courts have recognized a 4th Amendment right to extend even to those living in a homeless camp on

---

[49] Adnan Durakovic & Sabina Durakovic, "Regulating the Non-Military Use of Drones and Protection of Privacy" (2020) 58:3 J Crimin & Crim L 39 at 41.

public property.[50] Canada recognizes an inherent right to privacy but thus far there have been no cases on a reasonable expectation of privacy for the homeless in public spaces.

In China, the police are an extension of the state, and of state policy. It is well known that China is employing a vast network of video surveillance linked to artificial intelligence system. China maintains a national database with 300,000 criminal faces but they also track "mental illnesses, records of drug use, and those who petitioned the government over grievances." According to *The New York Times*, China is using some of these systems to supress citizens based on their ethnicity. A Chinese tech investor in AI who spoke with *The New York Times* said that "China has an advantage in developing [AI] because its leaders are less fussed by 'legal intricacies' or 'moral consensus.'" China is using artificial intelligence to track the approximately 11 million Uighur Muslims, of which nearly 1 million have been displaced into camps.[51]

China may be a cautionary tale about the use of facial recognition AI programs, but they are a state with numerous human rights violations and no right to individual privacy. This technology is potentially a tremendous tool to aid law enforcement and protect against terrorism. The problems with the technology do not come from the equipment, but the users. AI has not crossed into self-instruction apart from the influence of the programmer. In China, the bias of the state against their Uighur population influences the characteristics that the machine is looking for. "Results generated from these [software] calculations may appear like an objective science, but closer analysis reveals this technology's foundational reliance on observational biases that are crystallized into the enforcement records used to train this technology."[52] This type of bias is unavoidable and must be overseen by an independent agency to remove both the state and law enforcement from even perceived improper influences.

In the United States, following the January 6th, 2021 riots at the U.S. Capitol, technology played a crucial part in the charges laid stemming from that date. As of one year from the date of the riot, investigators have combed

---

50 See *State v. Pippin*, 200 Wn App 826.5

51 See Paul Mozur "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority", *The New York Times* (14 April 2019) online: <www.nytimes.com> [perma.cc/LQ4U-KWHX].

52 Shawn Singh, "Algorithmic Policing Technologies in Canada" (2021) 44:6 Man LJ 245 at 246.

through more than 20,000 hours of video and 15 terabytes of data. Over 725 people have been arrested. 145 people have pled guilty to misdemeanors and 165 of have pled guilty to felonies.[53] Beyond the tools available to investigators, there was a huge swell of public involvement in the investigation as the FBI listed photos and video of people wanted for the riot.[54]

Many people who respect privacy rights and are uneasy about state surveillance can be rallied in times of exceptional circumstance. Following events like 9/11 and the U.S. Capitol riots, people rallied behind government action such as the FBI call for online sleuthing into riot participants. Megan Ward states: "A state can prime and prep its citizens to accept otherwise distasteful breaches of personal privacy and rights through the opportunity to take matters into their own hands and enact justice against those they deem guilty."[55] It is easier to rally the public behind the apprehension of organizations or people with distasteful views. Online public consciousness is not a great example of sober reflection on the consequences of dangerous surveillance precedents. When it comes to pursuit of fanatics or those who seek to do harm, the posse mentality often quickly morphs into a lynch mob mentality.

Fundamental justice is an important concept to democracy and when the values of a society are ignored because of distasteful actions by a group within that society a precedent has been set and the risk of improper use of that technology dramatically increases. Of course none of these concerns need be a barrier to using technology to safeguard society. However, they are a sober reminder that the human rights of the distasteful elements of our society must be protected to effectively safeguard the human rights of the entire society.

C. Warrant Process

There is a higher duty than has been defined by the courts and legislation. Police are a public entity, composed of members of the public who have been entrusted with authority to serve the public good. Tools that

---

53 See Ryan Lucas "Where the Jan 6 insurrection investigation stands, one year later", *NPR* (6 January 2022), online: <www.npr.org> [perma.cc/D2ZP-UVRU].

54 See "Most Wanted: US Capitol Violence" (last visited 15 April 2022), online: *FBI Most Wanted* <www.fbi.gov/wanted/capitol-violence> [perma.cc/L8KY-92Z7].

55 Megan Ward, "Participatory Security and Punitive Agency: Acclimation to Homeland Surveillance in the United States" (2021) 19:3 Surveillance & Society 346 at 346.

can make law enforcement more effective and accurate should be zealously pursued. There is already a process in place for the state to intrude on recognized private grounds under the supervision of the judiciary. When it comes to surveillance, "only where those state examinations constitute an intrusion upon some reasonable privacy interest of individuals does the government action in question constitute a 'search' within the meaning of s. 8"[56]

The state must take every effort to distance themselves from intrusion upon the privacy of the public. A warrant-like process is the most ideal measure to allow expansion of state surveillance while protecting the public interest. The courts have struggled to define the concept of a reasonable expectation of privacy in a public sphere and it may be that there does not need to be an expectation of privacy if the access to that information has a gatekeeper.

Technology is increasing surveillance capability and decreasing price at a tremendous rate. Given some of the abilities discussed above, it is truly frightening how low the expectation of privacy should be. There are no serious concerns with the ability of a police officer to physically surveil a suspect. Even wiretaps or video surveillance used by an officer, which may capture unintended suspects, are not considered to be an invasion of privacy. Somehow the idea of an officer in control of technology for the purposes of surveillance does not trigger much suspicion, but automation is a different story.

D. Harmonizing Police and Technology

The use of modern surveillance, through increased cameras, drones, and artificial intelligence, evokes images of complete state surveillance. The police are not a machine of the state or controlled directly by any political body. Civilian oversight exists to ensure that the police function as members of the public to serve the public interest. Improved efficiency does not need to change the essential character of police activity. A video camera no longer requires any human monitoring to be able to function. This frees an officer up to engage with the public or respond faster to other needs.

Technological advancement cannot be stalled and as was mentioned above, even if the public decided that the police should not have access to these improved methods of surveillance, it is not possible to prevent the

---

[56] "In the Face of Danger: Facial Recognition and the Limits of Privacy Law", Note, (2007) 120:7 Harv L Rev 1870.

explosion of privately used surveillance currently happening. Police should have access to every technology that makes their job more efficient. The key though must be similar to the civilian police boards which act as a buffer between politicians and police. All technology that mass-captures the public and evaluates criminal activity must be managed through non-police, non-state entity.

Modern evidence-based police methods now rely heavily on surveillance footage for good reason. Proliferation of cameras does not need to be dystopian. If all footage and artificial intelligence evaluation were done outside of the police through an independent organization, then police could still have access to any and all relevant evidence, but would need to justify that access. To conduct specific surveillance, or obtain personal biometric identification information, a warrant should be needed.

Police must demonstrate that the information is related to a specific offence or that there is a reasonable likelihood to believe that someone has or will commit an offence. Mass surveillance should be the exact same procedure. When a crime is committed, it is in the public's interest to have criminals accurately and efficiently punished. Police should be able to apply for a warrant for a relevant search of public surveillance, and even tracking data from suspects.

Technology is not the problem with mass surveillance, but rather who has access to it. Society widely accepts that there is no expectation to privacy in the public sphere but expects that they will not be always scrutinized. Many people consider themselves to be responsible drivers, but they occasionally speed or drive with diminished attention to the road. We play with probability in our everyday lives and surveillance by police is acceptable to most people because of the idea that it is primarily focused on someone criminal, not them. Mass surveillance and scanning faces does not have to compromise this perception. It is entirely possible that we could venture out of our homes in confidence if we understood that the information being compiled about us was not accessible without oversight.

In a time where public perception of police has much controversy, technology should be welcomed rather than feared. Police should be protected from public perception through oversight, as much as the public would be protected from improper surveillance. It is not a far stretch to consider what else in the justice system would shortly become automated, following the adoption of artificial intelligent surveillance.

If a system could observe and document the commission of a crime, then suspects would quickly be convicted. There would be a greatly decreased need of a long pre-trial process to determine guilt when a machine could produce a report and evidence before the suspect was even picked up. Imagine a defence lawyer whose task was simply to look for any reasonable doubt to launch an appeal of an automated conviction, rather than to rely on introducing doubt to a jury of peers.

It is no longer science fiction to consider this type of a justice system where people are increasingly removed from operational decisions in the name of efficiency.

V. CONCLUSION

Technology is ever improving and becoming cheaper to use. Policing reform has been a controversial topic and the increasing use of surveillance by the police without a clear oversight regime does not foster transparent policing. It is clearly in the best interest of society to use every technology possible to protect people. Mass facial recognition and artificial intelligence can be employed under the watchful eyes of the court to ensure that no one state body has control over the data which is public life. Implementing an oversight regime and a warrant procedure will accomplish the goals of effective policing and privacy in our society.