

Body Worn Cameras (BWCS): Privacy Versus Solid Evidence

STANISLAVA ZGUROVA *

ABSTRACT

This paper will explore the dichotomy between the privacy concerns associated with the use of Body-Worn Cameras (“BWCs”) by law enforcement agencies, and the benefits associated with this technology, such as the evidential value of the BWCs video, audio, and images as reliable forms of evidence assisting courts and criminal justice players in making substantiated decisions and reaching just verdicts. The paper will provide a background overview of BWCs and the approach to their use in some Canadian jurisdictions, followed by a discussion on Canada’s struggles guarding the privacy of Canadians and the recent breaches of privacy conducted by the Royal Canadian Mounted Police (“RCMP”). Next, there will be a case-study section exemplifying the numerous flexible features and benefits of BWCs and produced digital evidence used in courts and police operations, followed by a section addressing the rule of law and the need for punishing police misconduct for mishandling highly sensitive information (such as that captured by BWCs). Lastly, the paper will reflect on its findings, discuss existing tensions, and propose a path forward for the safe and broad implementation of BWCs across Canada.

* Third year law student at the University of Manitoba, Faculty of Law. I obtained my Bachelor of Arts degree in Law and Society (with minor in German Language) in 2014 from the University of Calgary. I would like to sincerely thank Professor John Burchill for his invaluable support with the writing of this paper and for inspiring me to research the subjects of policing and privacy in depth. Many thanks also to the anonymous peer reviewers for their comments and feedback in the earlier stages of this paper, as well as the editors of the Manitoba Law Journal. All views (and errors) expressed here are my own, unless otherwise indicated.

Keywords: Body-worn cameras (BWCs); privacy; evidence; justice; transparency; accountability.

“Few things are as important to our way of life as the amount of power allowed the police to invade the homes, privacy and even the bodily integrity of members of Canadian society without judicial authorization.”¹

I. INTRODUCTION

BWCs are a highly effective tool assisting not only police operations but also the public and the judicial system in the pursuit of fairness, transparency, and justice. Analogous BWCs digital evidence-gathering policies and practices should be employed collaboratively across jurisdictions. With this new technology, however, there are hidden risks of compromising an individual's privacy. Therefore, to mitigate that risk, law enforcement agencies across the country must adhere to the highest standards of privacy protection and only gather the information needed for specific police encounters or investigations. Strict measures guarding the use of digital information collected through BWCs must be in place at each police agency, regulated and enforced internally and externally. Digital data is easily abused and disseminated. The content of the information gathered through BWCs is highly sensitive as it contains large amounts of private information about Canadians, often exposing them to vulnerable circumstances.

Canadians enjoy constitutionally protected freedoms and liberties worth stringent protection measures applicable uniformly across the country. Hence, police services equipped with tools capable of producing invaluable evidence and allowing respective courts to rely on a steady process when resolving criminal cases are key in ensuring that those rights and freedoms are consistently protected. BWCs also allow for transparency and accountability in the relationship between the police and the public, especially in cases involving complaints about the police's use of excessive force. In short, the diverse standards and policies of BWCs among law enforcement agencies across Canada yield unequal protection of fundamental rights and freedoms for Canadians and less substantiated and less reliable outcomes of criminal cases. To date, there are more Canadian law enforcement agencies without BWCs than ones that use them in their

¹ The Honourable Justice Binnie in *R v Tessling*, 2004 SCC 67 at para 13.

daily operations, and this should change. BWCs should become a regular component of the equipment of front-line police officers across the country, especially when policing urban and high-density population areas.

On the one hand, the RCMP's rollout of their BWCs implementation project could be viewed as an example of a crucial step in the right direction towards achieving uniformity and consistency in policing across Canada. Now, all front-line RCMP officers will be equipped with BWCs. However, given that the RCMP is usually contracted in rural or remote areas within the provinces, this will likely lead to major differences in policing practices within the same provincial jurisdiction. Such disparity will be especially palpable in provinces like Manitoba, where BWCs are not widely adopted. Consequently, certain individual jurisdictions within the province, with their corresponding criminal justice players, will have access to and could benefit in their decision-making from the high-definition digital evidence BWCs are capable of producing, while others will not. This discrepancy in access leads to a concerning double standard of policing and decision-making within a province and across all Canadian jurisdictions. Hence, the ability of jury members, judges, and Crown prosecutors to hear and see the recording of disputed police interaction with an accused person, as opposed to assessing the credibility of *viva voce* evidence by each side in the dispute, will streamline court process and decision-making and lead to more transparent and reliable just outcomes.

Crown prosecutors, judges, juries, members of the public, and police officers in each part of Canada deserve equal access to the same effective tools assisting their work and the pursuit of justice. Therefore, BWCs should be widely implemented across Canada in a unified manner. It is speculative whether the RCMP's initiative will positively influence local police agencies to adopt BWCs in their operations to keep up with the federal policing standards embodying the values of transparency and accountability (and maybe even compete with them) or if it will have the opposite effect and discourage police agencies from BWCs adoption to avoid challenges the technology may present. Only time will tell how that trend progresses.

II. BODY-WORN CAMERAS (BWCs) OVERVIEW

A. General Background on BWCs

Regulating officer-citizen interactions via BWCs is founded upon the logic behind Jeremy Bentham's theory of the Panopticon, where (the prison) population's behavior is altered through transparent and constant monitoring as opposed to the use of force. However, such a modern technological surveillance strategy sacrifices privacy for everyone "under the gaze" – police officers and the public recorded on the BWC.² Hence, BWCs "pit the two revered democratic values of privacy and transparency against each other."³

The United Kingdom ("UK") was the first nation to employ the use of BWCs in its front-line police operations in 2007 after allocating £6 million for the implementation of the project. The United States of America ("USA") was the second nation that mass deployed BWCs in its police forces. Under President Obama, the Department of Justice dedicated over \$32 million to adopting BWCs across the USA.⁴ This was in response to the eruption of protests over questionable police practices leading to the coalition of multiple civil rights groups, whose leaders called for BWCs implementation by police forces "to pierce opacity and improve accountability and transparency."⁵ The first and most notable national protest that sparked the shift towards the mass adoption of BWCs in American policing was over the death of Michael Brown, an unarmed teenager shot in Ferguson, Missouri, by a police officer responding to a call for a convenience store theft. The protesting civil rights and liberties groups saw BWCs as "a way to monitor the police, promote accountability, and reduce the risk of injuries and death in police encounters."⁶ Furthermore, police chiefs also recognized the benefits BWCs could provide, such as offering evidence, rebuilding trust, reducing unfounded complaints, and potentially exonerating police officers.⁷ Hence, BWCs today have become

² Mary D Fan, "Privacy, Public Disclosure, Police Body Cameras: Policy Splits" (2016) 68:2 Ala L Rev 395 at 407.

³ *Ibid* at 412.

⁴ *Ibid* at 399, 419.

⁵ *Ibid* at 398.

⁶ *Ibid* at 410.

⁷ *Ibid*.

part of the equipment of police officers in most developed countries, and Canada is still catching up.

Even before the significant shift of deploying over 2000 BWCs in the field, the UK had one of the world's most extensive video surveillance systems amounting to more than four million close-circuit cameras.⁸ Originally in the UK, the direction for officers wearing BWCs was to conduct nearly continuous recording. However, there has been a departure from that practice towards BWCs recording based on the officer's discretion.⁹ Today, one of the major worldwide BWCs policy debates is on this point – how much discretion should police officers wearing BWCs have in deciding when to record and when not to?¹⁰ This discretion is directly related to the levels of police accountability and transparency the BWCs are meant to enhance.

Another debate surrounding BWCs policies is who should bear the burden of asking for or allowing recordings. Should the officer be expected to ask for permission, or should the public – victims and witnesses interacting with the officer – request that recording ceases? Mary Fan argues that it is “unrealistic to expect the public to order a police officer to stop recording, especially after a traumatizing or high-stress experience.”¹¹ Moreover, the public should be allowed to maintain control over whether an individual should be recorded by a BWC, as opposed to having the burden to speak out and express that they do not wish to be recorded.¹² Hence, as the author asserts, the hidden price of the benefit of BWCs should not be the infliction of further privacy harm on those who seek help.¹³ The same tensions and issues live in Canada, where each police jurisdiction adopts its policies and takes an individual approach toward the degree of control and autonomy displayed within officer-citizen interactions. An overview of some BWCs policies follows in sub-section B.

So how effective, if effective at all, are BWCs in regulating officer-citizen interactions? Numerous studies have been conducted, mostly in the USA, exploring various issues and tensions arising from the use of BWCs and the community's perceptions of it. Some results are best described as

⁸ *Ibid* at 419.

⁹ *Ibid* at 422.

¹⁰ *Ibid* at 426.

¹¹ *Ibid* at 404.

¹² *Ibid* at 407.

¹³ *Ibid* at 404.

inconclusive, whereas the findings of others widely vary. For example, the *Campbell Systematic Review* compiled and analyzed data from thirty previously conducted studies on BWCs (mostly in the USA) and concluded that BWCs could reduce the number of public complaints against police officers.¹⁴ However, it is unclear whether this is a sign of improved interaction between the police and the public or a change in reporting. Furthermore, it was insufficient to conclude whether BWCs reduce officer use of force. The study also found that BWCs do not seemingly affect other police and citizen behaviours, including officers' arrest behaviours, self-initiated activities, dispatch calls for service, and assaults or resistance against police officers. Lastly, there is no firm conclusion regarding the overall expectations that BWCs might have an impact on officer or citizen behaviours.¹⁵

Another much narrower BWCs study conducted in two police districts in Florida aimed to gather participants' perceptions on potential benefits and privacy concerns surrounding the use of BWCs. Respondents highly agreed that BWCs are generally beneficial. More specifically, participants agreed that BWCs improve the following: officer's and resident's behaviour, views on police legitimacy, and the collection of quality evidence. Interestingly, respondents were not very concerned about privacy implications arising from the use of BWCs.¹⁶ Hence, it is evident that the BWCs effects on transparency and accountability are unverified by concrete, substantial research statistics.

These inconclusive statistical results about whether BWCs affect officer's behaviour, improve officer-citizen interactions, and reduce the use of excessive police force are exemplified by the events surrounding the death of George Floyd on May 25, 2020, in Minneapolis, Minnesota, when he was reported to have used a counterfeit \$20 bill at a convenience store.¹⁷ Unfortunately, all six police officers responding to the complaint call were

¹⁴ Cynthia Lum et al, "Body-Worn Cameras' Effects on Police Officers and Citizens Behaviour: A Systematic Review" (2020) 16:3 *Campbell L Rev* 1 at 3.

¹⁵ *Ibid.*

¹⁶ Matthew S Crow et al, "Community Perceptions of Police Body-Worn Cameras: The Impact of Views on Fairness, Fear, Performance, and Privacy" (2017) 44:4 *Criminal Justice and Behaviour* 589 at 600.

¹⁷ Evan Hill et al, "How George Floyd Was Killed in Police Custody" (31 May 2020), online: *The New York Times* <www.nytimes.com/2020/05/31/us/george-floyd-investigation.html> [perma.cc/3A83-N9LV].

wearing BWCs, yet that did not alter their behaviour nor prevent them from committing a series of steps in violation of Minneapolis Police Department policies when responding to the incident and ultimately caused Mr. Floyd to suffocate and die while in police custody.¹⁸ Nonetheless, even though BWCs did not prevent the officers, Derek Chauvin in particular, from applying continuous excessive force over a long period of time over Mr. Floyd, their footage assisted in the investigation of the incident and provided a neutral, observational lens allowing the internal investigation and subsequently the court to comprehend how the events unfolded. Hence, BWCs were of great assistance in the legal proceedings as reliable pieces of evidence, and their existence and use embodied the values of police transparency and accountability.

Lastly, a 2018 study on the public's perception of police conduct depicted in BWCs footage posted on a specific American YouTube channel found that media's labeling and description of incidents, as well as embedded video comments and voice narration, can have an impact on public's perception of police conduct and the specific police-citizen interaction captured on the BWC video. The effects of the embedded comments and narration in the BWC video are subsequently reflected in the viewers' comments attached to that YouTube post.¹⁹ While in Canada, BWC videos are subject to strict privacy regulations and are not posted on social media platforms, it is important to note the findings of that study and attribute the influence of social media in shaping the narrative about BWCs and police-citizen interactions.

B. BWCs in Canada

In Canada, following the 2007 RCMP in-custody death of Robert Dziekanski, who was an immigrant detained at the Vancouver airport, and who was tasered and allegedly died from it, a conversation about BWCs began by acknowledging the need "to see and hear the event unfold through the eyes and ears of the officer at the scene."²⁰ It is important to note,

¹⁸ *Ibid.*

¹⁹ Christopher J Schneider, "An Exploratory Study of Public Perceptions of Police Conduct Depicted in Body Worn Camera Footage on YouTube" (2018) 7 Annual Rev Interdisciplinary Justice Research 118.

²⁰ Canada, Home Office (Police and Crime Standards Directorate), *Guidance for the Police Use of Body-Worn Video Devices*, (Chair of the Civilian Review and Complaints Commission for the RCMP in 2009 Report Following a Public Interest Investigation into a Chair-Initiated Complaint Respecting the Death in RCMP Custody of Mr.

however, that while it is true that there is a need for an objective and neutral lens in a circumstance like this, which the BWCs can provide, the advancement of technology since that statement was made has led to concerns that one should keep in mind when viewing a video and audio recording captured via a BWC. More particularly, in June 2021, the Information and Privacy Commissioner of Ontario issued a Model Governance Framework for Police Body-worn Camera Programs in Ontario, where it was highlighted that “[p]olice services need to determine the appropriate video resolution and audio quality being captured by the BWCs. The video and the audio of some cameras can substantially outperform what the human eye and ear can perceive.”²¹ Therefore, two major concerns arise from this high capability of some BWC devices. One, there are apprehensions regarding breaching the privacy of individuals not related to the incident but are captured without providing consent simply because of their mere presence in the vicinity of the BWC recording. Hence, the BWC devices and supporting software chosen by the police force should provide features allowing management and manipulation of the digital data: such as blurring and voice distortion, to protect individuals’ privacy.²² The other major concern regarding reviewing recordings captured by a high-definition BWC device is the incorrect assumptions that may be made by the viewers, who will likely equate what is heard and seen on the recording with the human perception of the officer wearing the BWC, which may differ from that of the actual recording.²³ Therefore, the safest route to address these two concerns is to use devices that resemble human capabilities more closely, as opposed to very high-definition BWCs.

The need for police forces to equip themselves with BWCs was also addressed in a 2014 report completed for the Toronto Police Service on the issues surrounding police responses to mental health calls and encountering people in crisis. Justice Iacobucci recommended the implementation of BWCs in the operations of the Toronto Police Service by stating that they

Robert Dziekanski) at 5.

²¹ Information and Privacy Commissioner of Ontario, “Model Governance Framework for Police Body-worn Camera Programs in Ontario” (2021) at 5, online (pdf): <www.ipc.on.ca/wp-content/uploads/2021/07/model-governance-framework-police-body-worn-camera-programs.pdf> [perma.cc/3SG6-MDPF] [Model Governance Framework Ontario] [emphasis added].

²² *Ibid.*

²³ *Ibid.*

should be issued to “all officers who may encounter people in crisis to ensure greater accountability and transparency for all concerned.”²⁴ Additionally, the usefulness of video evidence generated by police had, at the time, also been addressed by Canadian courts. In *R v Hughes*, the Ontario Court of Justice relied on ICDV evidence in a case involving drinking and driving charges.²⁵ The court stated that “[s]imply put, the [in-car] camera video is the best evidence of the offence, essential not only to possible *Charter* motions but also to the applicant’s ability to make full answer and defen[c]e.”²⁶ In its decision, which granted a stay of proceedings remedy due to an unreasonable delay of the Crown’s disclosure to the defence and the difficulties the defence faced with the format of the digital recording, the court also acknowledged the following:

The police have elected to improve their methods of investigation through the use of technological advances. This is laudable and consistent with the public interest that the Court has before it the best evidence capable of exonerating or inculcating an accused person. That being said with these advances, comes the responsibility of the State to insure that the accused has proper access to the disclosure.²⁷

Lastly, the implementation of BWCs in police force operations requires the planning and development of a Digital Evidence Management System (“DEMS”), which is defined as a “software application that allows for the secure uploading, storage, and retrieval of digital files in various data formats.”²⁸ DEMS are offered by private sector vendors and includes cloud-based platforms.²⁹

C. BWC Regulations in British Columbia (“BC”)

BC was one of the first Canadian provinces to conduct pilot projects on BWCs, dating back to 2009. The most known pilot project was with the Victoria Police Department, where 20 officers were involved in testing two different types of BWC devices. Although mixed and inconclusive, the

²⁴ Ontario, Toronto Police Service, An Independent Review Conducted by the Honourable Frank Iacobucci for Chief of Police William Blair, “Police Encounters with People in Crisis”, (July 2014) at 263.

²⁵ *R v Hughes*, 2014 ONCJ 105 [Hughes].

²⁶ *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982 (UK)*, 1982, c. 11 [Charter]; *Ibid* at para 44.

²⁷ *Hughes*, *supra* note 25 at para 54.

²⁸ Model Governance Framework Ontario, *supra* note 21 at 2.

²⁹ *Ibid*.

results supported the further use of BWCs and summarized BWCs as well-received technology by police officers, the public, and the Crown.³⁰

Prior to BWCs being “deployed” in the police operations field, a privacy impact assessment must be conducted and approved by the “appropriate head of the public body.”³¹ This has been the practice in all Canadian jurisdictions where BWCs have been tested and/or launched. An appropriate policy needs to be implemented to address issues such as the purpose of the program, the circumstances that BWCs will be turned on and off, the amount of time to retain the BWC videos, and the accessibility of BWC videos. Furthermore, the policy must also specifically address the procedures for processing, storing, accessing, and reviewing BWC videos, as well as specific procedures surrounding the access requests for BWC videos and ensuring adherence to applicable provincial or federal privacy legislation if the BWC video is disclosed.³²

Moreover, training must be provided to officers on how to use the BWCs properly. Full, automatic, and continuous recording is discouraged according to the BC BWC Provincial Policing Standards. The same direction is also exhibited in the current RCMP BWC Policy and the Calgary Police Service BWC policy and Standard Operating Procedures (“SOPs”).³³ The caveat to that is the mandatory recording of police use of force and violent or aggressive behaviour encounters. Single incidents are to be recorded in their entirety subject to exigent circumstances requiring the deactivation of the camera, and officers must not delete BWC videos.³⁴

³⁰ Edmonton Police Service, “Body Worn Video: Considering the Evidence: Final Report of the Edmonton Police Service Body Worn Video Pilot Project” (June 2015), online (pdf):

<bj.a.ojp.gov/sites/g/files/xyckuh186/files/bwc/pdfs/EdmontonPS_Canada_BWVFinalReport.pdf> [perma.cc/MR8Y-GUQK].

³¹ British Columbia, “Equipment and Facilities: Body Worn Cameras” (01 July 2019) at s 1, online (pdf): *Provincial Policing Standards* <www2.gov.bc.ca/assets/gov/law-crime-and-justice/criminal-justice/police/standards/4-2-1-body-worn-cameras-equipment.pdf> [perma.cc/DWP6-Q6FP] [BC BWCs policy].

³² *Ibid*, s 3.

³³ *Ibid*, s 5; Canada, Royal Canadian Mounted Police, OM – ch 25.5 *Body-Worn Camera*, (Policy) (Ottawa: RCMP 2022, retrieved via email: BWC_policy_politique_CVC@rcmp-grc.gc.ca) [RCMP BWCs policy]; Alberta, Calgary Police Service, *Body Worn Cameras Ref #IN007-1*, (Policy) (Calgary: CPS Bureau of Community Policing, September 2015) [CPS BWCs policy].

³⁴ BC BWCs policy, *supra* note 31, s 10.

Reasons for the failure to record an incident or to deactivate the BWC prior to the conclusion of the incident must be articulated in the officer's notes or report within 12 hours after the shift ends.³⁵ The BC Provincial Policing Standard also emphasizes that BWC videos do not replace officers' notes and reports, and police officers using BWCs should continue to write in accordance with existing policies.³⁶ The same approach is also adopted by the RCMP and Calgary Police Service ("CPS"), where it is explicitly emphasized that BWC recordings do not replace existing officer note-taking practices. Security and access to BWC videos is another important aspect of the BC Provincial Policing Standard, and it is limited to only authorized persons having access to them for investigative, training, or internal audit purposes.³⁷ Officers in the field cannot alter BWC videos.³⁸ BWC videos are also subject to internal audits where a random sample of BWC videos is selected to ensure compliance with the implemented policies and procedures pertaining to secured storage, deletion of videos, and unauthorized viewing.³⁹

D. RCMP's BWC Operational Policy

In October 2022, the RCMP rolled out a policy to implement BWC in their operations at each service location.⁴⁰ Between 10,000 – 15,000 RCMP members, who interact with communities across rural, urban, and remote locations in Canada, will be equipped with BWCs. The project aimed at strengthening transparency, accountability, and the public's trust in the federal police, in the improvement of police and public behaviour, in evidence gathering, and in resolving public complaints.⁴¹ Alberta, Nova Scotia, and Nunavut are the first three RCMP divisions where field tests have been conducted, followed by the implementation of BWCs across Canada in the subsequent 18 months.⁴²

³⁵ *Ibid.*, s 13.

³⁶ *Ibid.*, s 14.

³⁷ *Ibid.*, ss 15, 17.

³⁸ *Ibid.*, s 16.

³⁹ *Ibid.*, s 25.

⁴⁰ Royal Canadian Mounted Police, "Body Worn Cameras" (27 October 2022), online: *Royal Canadian Mounted Police* <www.rcmp-grc.gc.ca/en/body-worn-cameras> [perma.cc/PGH7-6LMM].

⁴¹ *Ibid.*

⁴² *Ibid.*

According to the RCMP BWC policy, a BWC is “an approved RCMP device that is worn on a designated member’s uniform in an overt capacity for the main purpose of recording audio and/or video.”⁴³ The general purposes of RCMP BWCs are to capture an accurate record of the members’ interaction with the public, enhance public safety and officer safety, provide improved evidence for investigative, judicial, and oversight purposes, and enhance bias-free service delivery.⁴⁴ The RCMP BWC devices will be equipped with audio and video indicators (lights), which serve as visible signals to individuals the officer interacts with and the public that they are being recorded.⁴⁵

Nevertheless, the BWC also has a feature of operating in “covert mode,” which disables these indicators and allows the BWC to record events in secret.⁴⁶ While it is questionable whether a BWC can be operated in “covert mode” without a “one-party” consent judicial authorization under s. 184.2 of the *Criminal Code* or when it is used for officer safety purposes under s. 184.1; it is possible the RCMP takes the position anyone talking with a police officer should not consider their communications private. Therefore, the officers have the sole discretion in enabling the covert mode, but if done often, this may undermine the public’s trust in police, not enhance it. Additionally, RCMP BWC videos are subject to redactions, which is “[the] deliberate omission or concealment of information in a multimedia recording. Redaction involves removing sensitive or personal information from data, such as documents, audio files, and videos.”⁴⁷

Furthermore, as specified by the Information and Privacy Commissioner of Ontario, the methods of BWC activation are another important consideration when implementing BWC policy and police operations. Such activations can be manual or triggered upon the activation of a sensor.⁴⁸ Sensors can be placed in the police vehicle’s light bar or siren or the officer’s firearm holster, and the activation of the camera can be automatic each time the sensor is triggered upon turning on the lights or sirens of the police vehicle or each time the officers draw their weapons. Additionally, BWC has the “capacity to record the exact date, time, and

⁴³ RCMP BWCs Policy, *supra* note 33, s 1.1.

⁴⁴ *Ibid*, s 2.1.

⁴⁵ *Ibid*, ss 1.6, 4.3.

⁴⁶ *Ibid*, ss 1.6, 4.2.

⁴⁷ *Ibid*, s 1.14.

⁴⁸ Model Governance Framework Ontario, *supra* note 21 at 6.

location of when and where they begin recording.”⁴⁹ The RCMP BWC Policy does not address any of these aspects of BWCs. At this moment, it is unclear whether any of these features would be utilized. The current policy only specifies that RCMP officers have the discretion to start and stop recording manually and determine whether to use covert mode.

The RCMP BWCs will also utilize a pre-event video recording function, allowing the device to capture the 30 seconds before its activation and attach it to the subsequent video.⁵⁰ The Information and Privacy Commissioner of Ontario points out that the capability of some BWCs pre-event recording allows for a better context of the video and audio recording by capturing the events leading to the activation of the camera.⁵¹ On the one hand, this is a great safety feature of a BWC device, allowing for a better context of events and enhancing transparency and accountability in the interaction between an officer and a member of the public. On the other hand, however, the mechanism behind that feature raises privacy concerns since the BWC is constantly passively recording, regardless of whether it is on or off. This raises the question of what happens to the passively captured data while the BWC is off. Such recording would likely not end up on the cloud-based storage or DEMS since it is not part of actual footage. Does the vendor then store this information, and if yes, what does the vendor do with it? Is this potential use of private information and breach of privacy regulated, and if yes, how?

Next, the RCMP BWC Policy outlines that only trained RCMP officers are authorized to wear BWCs, and they can exercise their discretion as to where, when, and how to record. More specifically, the policy outlines that officers may choose to record only in audio, video, or covert mode. In such instances, a reasonable explanation detailed in the officer’s notes is required.⁵² Furthermore, RCMP officers are expected to respect the reasonable expectations of privacy at dwellings, hospitals, and religious places.⁵³ When entering private spaces with consent (as opposed to a search warrant or exigent circumstances), RCMP officers are to advise the owners or occupants of the recording and provide them with a “reasonable

⁴⁹ *Ibid.*

⁵⁰ RCMP BWCs policy, *supra* note 33, s 1.13.

⁵¹ Model Governance Framework Ontario, *supra* note 21 at 6.

⁵² RCMP BWCs policy, *supra* note 33, s 4.3.

⁵³ *Ibid.*, s 1.11.

opportunity to refuse or consent to being recorded.”⁵⁴ Interestingly, the BWCs policy directs RCMP officers to “when possible, avoid unnecessary recording audio and/or video data.”⁵⁵ Arguably, this direction unnecessarily broadens the scope of an officer’s discretion. How does an RCMP officer assess what is necessary and unnecessary in the field, especially in fast-paced situations? Will this lead to the omission of significant events and interactions that should have been captured on the BWC but were not? It is also important to note that according to the RCMP BWCs policy, BWCs videos “are not subject to biometric analysis including, but not limited to, facial recognition.”⁵⁶ Other BWC policies and guidelines are silent on this point. Does that mean that in those jurisdictions, the BWCs videos are subject to biometric analysis?

Additionally, the RCMP policy calls for close supervision of officers equipped with BWCs and emphasizes that the BWC video and audio footage “does not replace proper note taking or reports.”⁵⁷ Moreover, supervisors are directed to “[i]nspect members’ notebooks regularly to ensure the continuing quality of note-taking with the use of the BWC.”⁵⁸ Additionally, prior to reviewing BWC recordings, RCMP officers are required to submit a written request, and upon review of the video, if there is an additional detail not previously observed yet now added to the officer’s written notes, a notation for the inclusion is supposed to be made.⁵⁹ As a general rule, the RCMP BWC policy points out that videos should “complement, but not replace, evidence from other sources, such as police officers, witnesses, or evidence that is not normally captured by Forensic Identification Services.”⁶⁰ Furthermore, the BWC video “does not replace existing requirements, procedures, or policy obligations, such as recording admissions, statements, or declarations.”⁶¹ Curiously, an RCMP BWC is not used as a “routine performance evaluation tool.”⁶² Perhaps, this

⁵⁴ *Ibid*, s 4.2.2.

⁵⁵ *Ibid*, s 3.1.6.

⁵⁶ *Ibid*, s 2.9.

⁵⁷ *Ibid*, s 5.1.

⁵⁸ *Ibid*, s 3.2.4.

⁵⁹ *Ibid*, ss 5.2–5.3.

⁶⁰ *Ibid*, s 5.4.

⁶¹ *Ibid*, s 5.5.

⁶² *Ibid*, s 3.2.

technology could be better utilized in future practices towards evaluating officers' performance and addressing gaps in training.

It must be stressed that the government cannot unilaterally collect and manage the private information of Canadians. Hence, federal statutes applicable to the RCMP BWC policy exist to allow private citizens and permanent residents to request and view the information gathered via BWCs worn by RCMP members when the interaction in question occurred. Similar provisions and policies assisting private citizens and permanent residents in accessing BWC video and audio recordings from any local police service can be found in provincial legislations. The two pieces of federal legislation providing mechanisms for access to BWCs video and audio recordings are *The Access to Information Act* and *Privacy Act*.⁶³ They are also referenced in the RCMP BWC policy under section 3.4.

As outlined in the *Access to Information Act*, any Canadian citizen or permanent resident can submit a request to access the BWCs video, as per sections 4(1) and 6. However, access is not guaranteed as per the statute, and the "head of the government institution" has discretion and can "decline to act in the person's request if, in the opinion of the head of the institution, the request is vexatious, is made in bad faith or is otherwise an abuse of the right to request access to records."⁶⁴ Moreover, s. 12(1) of the *Privacy Act* addresses the right of access of every Canadian or permanent resident to personal information about the individual contained in an information bank or in any government institution subject to the individual pinpointing the location of the information to assist the government in locating and retrieving it.⁶⁵ The requests to access personal information must be submitted in writing to the government institution containing it.⁶⁶ This requirement places a high burden on the individual applying for access to the information to know and list which government department has or may have the relevant personal data, which may potentially lead to incomplete disclosure due to the applicant's gaps in knowledge, especially in instances where more than one department may contain it.

In response to a written application for access to personal information by a private citizen (or a permanent resident), the head of the government

⁶³ *The Access to Information Act*, RSC, 1985, c A-1 [*The Access to Information Act*]; *Privacy Act*, RSC 1985, c P-21 [*Privacy Act*].

⁶⁴ *Ibid*, *The Access to Information Act*, s 6.1(1).

⁶⁵ *Privacy Act*, *supra* note 63, s 12(1).

⁶⁶ *Ibid*, s 13(2).

institution in possession of the information should, within thirty days from the submission of the written request, provide a written notice outlining whether or not access will be granted, and if approved, share the information.⁶⁷ Yet, similarly to the administrative procedure surrounding access to personal information as per *The Access to Information Act*, the head of the government institution has the discretion and may refuse to grant access upon stating the reasons for such refusal.⁶⁸ In such cases, the private citizen (or permanent resident) has the right to file a complaint to the Privacy Commissioner of Canada.⁶⁹

E. BWCs and Privacy Concerns in Calgary

In September 2015, CPS undertook and published a privacy impact assessment (“PIA”) for the project of adopting the use of BWC and In-Car Digital Video (“ICDV”) technologies in their day-to-day operations. In 2019, all front-line CPS officers and marked police vehicles were equipped with these new pieces of technology. Prior to this project, CPS worked collaboratively with the other UK and US jurisdictions that had already successfully implemented the use of BWC and ICDV. From the start, the PIA acknowledged that “[t]he use of this technology can be privacy-invasive.”⁷⁰ Consequently, since CPS is a public and provincial body, it must comply with provincial privacy legislation, specifically the *Freedom of Information and Protection of Privacy Act* (FOIP), and the Alberta Information and Privacy Commissioner oversees this compliance.

The main goal of the PIA was to address risks and privacy issues flagged by Privacy Commissioners across the country and illustrate the appropriate measures for CPS to undertake to mitigate those concerns.⁷¹ Some of the previously raised privacy issues with BWC and ICDV technology included the following: whether they were the least privacy-invasive alternative for effective policing; the availability of appropriate general notification to the public, specifically to individuals recorded by the BWCs; constant recording vs. recording only for specific police-citizen interactions; implementation of

⁶⁷ *Ibid.*, s 14(a) and (b).

⁶⁸ *Ibid.*, s 16(1).

⁶⁹ *Ibid.*

⁷⁰ Alberta, Calgary Police Service, *Body Worn Cameras (BWC) and In Car Digital Video (ICDV)* (Privacy Impact Assessment), (16 September 2015) at 1 [CPS PIA].

⁷¹ *Ibid.*

appropriate measures to record bystanders; the availability of proper safeguards pertaining to the collection, use, and disclosure of personal information and regarding retention, storage, and destruction of BWC recordings; whether the captured BWC data will be subject to any CPS internal analysis and if yes, what type; will recorded individuals have proper access to BWC records; and will CPS have the appropriate policies and procedures to implement the project.⁷²

When conducting their research and assessing the pros and cons of the new technology, CPS relied on data gathered from the UK Home Office. The data demonstrated that the use of BWCs has increased the following: the number of domestic conflict resolutions, appropriate custodial sentences, public confidence, and the number of citizen complaints.⁷³ The storage media is securely stored within the BWC device and cannot be directly accessed by the officer wearing it.⁷⁴ There is also a centralized Court Disclosure Unit, and “only specially trained individuals will have access to the video for the purpose of creating a Disclosure package for the Crown.”⁷⁵ It is recommended that members continue to record “notwithstanding the objection as consent is not required when the recording occurs in the context of law enforcement and policing activities.”⁷⁶ This conservative and rigid approach to the continuous use of BWCs persists as per CPS policies and guidelines, even in private dwellings and places of worship and religion, and in response to calls involving highly sensitive matters such as domestic violence and sexual assault.⁷⁷

As noted in the CPS’s PIA, there are four key considerations concerning what constitutes a reasonable expectation of privacy: necessity, proportionality, effectiveness, and minimal intrusiveness. In the privacy analysis conducted by CPS prior to launching the use of BWCs and ICDV, these four privacy characteristics were addressed, along with how their BWCs policies can take steps towards mitigating such potential breaches. The rationale was that “[t]he use of officer notes and reliance on memory has been the long-standing reporting system for police officers.”⁷⁸ However,

⁷² *Ibid* at 1–2.

⁷³ *Ibid* at 5.

⁷⁴ *Ibid* at 15.

⁷⁵ *Ibid* at 16.

⁷⁶ *Ibid* at 10.

⁷⁷ *Ibid* at 10–11.

⁷⁸ *Ibid* at 22.

it is noted that an officer's memory can be "seriously flawed," as it was in Robert Dziekanski's case. In such circumstances, there is no better alternative to a BWC video that reveals the perspective and point of view of the officer involved.⁷⁹ Moreover, CPS undertook the approach of limiting the use of BWC to instances of public interactions invoking the discharge of their law enforcement and policing duties, as opposed to unnecessarily recording each public interaction.⁸⁰ BWCs are also not to be used when strip searches are conducted.⁸¹ Furthermore, the use of BWCs provides an opportunity for an alternative and neutral perspective on an officer-citizen interaction, as opposed to relying on potentially biased, one-sided officer's notes.⁸² Officers would consider recording with their BWCs "when safe and practicable to do so" in circumstances involving youth interactions or where the setting is bathrooms, changerooms, and other private spaces, and the occupants have a reasonable expectation of privacy.⁸³ Therefore, CPS took into account all aforementioned privacy issues and concerns related to BWCs (and ICDV) technology and concluded that there is no less intrusive alternative to achieving enhanced transparency and accountability in the relationship between the police and the public than the implementation of these new tools into front-line police operations.⁸⁴

F. 2021 Model Governance Framework for Police BWCs in Ontario

In June 2021, the Information and Privacy Commissioner of Ontario issued a BWC Model Governance Framework recommending that BWCs videos not be subject to artificial intelligence (AI) or biometric technology (including facial recognition), as well as used in conjunction with live streaming capabilities "until lawful authority for doing so is clearly established."⁸⁵ This, however, implies that the direction for the use of BWCs videos is headed towards it being subject to AI and facial recognition software. Therefore, the data gathered by BWCs may be easily cross-

⁷⁹ *Ibid.*

⁸⁰ *Ibid.*

⁸¹ *Ibid.*

⁸² *Ibid.*

⁸³ *Ibid.*

⁸⁴ *Ibid.*

⁸⁵ Model Governance Framework Ontario, *supra* note 21 at 2.

referenced with other databases (i.e., mug shot databases) and can be used to gather metadata and behavioural data on everyone captured in the field of view and sound of the BWC camera.⁸⁶ Further discussion on privacy concerns follows in Part III.

CANADA'S STRUGGLES WITH PRIVACY

Privacy can be defined as:

The state of desired "in access" or as freedom from unwanted access, with "access" meaning perceiving a person with one's senses, including hearing them or obtaining information about them. Thus, speaking theoretically, a person's privacy will be interfered with if another obtains, listens to, or finds out information about them against their wishes or enables others to do the same.⁸⁷

In February, 2021, the Office of the Privacy Commissioner of Canada and the Privacy Commissioners of Quebec, British Columbia, and Alberta conducted a joint investigation of Clearview AI, Inc. ("Clearview") and concluded that "Clearview engaged in the collection, use, and disclosure of personal information through the development and provision of its facial recognition application, without consent" and for inappropriate purposes.⁸⁸ Clearview failed to comply with a number of federal, provincial, and territorial privacy statutes and pieces of legislation and used "biometric information for identification purposes without the express consent of the individuals concerned and by not disclosing the database of biometric characteristics and measurements to the Commission."⁸⁹ The investigation recommended that Clearview stops offering facial recognition services to clients in Canada subject to the investigation; stops collecting, using, and

⁸⁶ *Ibid* at 1–2.

⁸⁷ John Burchill, "Special Issue: Criminal Law Edition (Robson Crim) Tale of the Tape: Policing Surreptitious Recordings in the Workplace" (2017) 40:3 Man LJ 247 at 278 [Tale of the Tape].

⁸⁸ Office of the Privacy Commissioner of 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 Privacy Commissioner of Alberta" (2 February 2022), online: *Office of the Privacy Commissioner of Canada* <priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/> [perma.cc/CH24-YWB6].

⁸⁹ *Ibid* at para 120.

disclosing images and biometric facial data from Canadians; and deletes images and biometric facial data collected from Canadians.⁹⁰

The events leading to this investigative report and recommendations are founded upon the revelations in 2020 that Clearview was expanding its facial recognition database by using images from public websites, among which Facebook, YouTube, Instagram, and Twitter, in violation of those websites' terms of service and without consent of individuals.⁹¹ Over three billion images with their corresponding biometric identifiers were obtained into Clearview's database - a large number of those images were of Canadians, including children.⁹² Additionally, at that time, reports confirmed that several Canadian law enforcement agencies and private organizations have used Clearview's services to identify individuals.⁹³

In June 2021, The Privacy Commissioner of Canada submitted a letter to the Speaker of the Senate addressing the findings from the earlier investigation on RCMP's use of Clearview services, specifically facial recognition technology ("FRT"), and drafted joint guidance for law enforcement agencies considering the use of facial recognition technology.⁹⁴ The commissioner acknowledged that FRT could have an effect on an individual's privacy and undermine rights, liberties, and freedoms, among which are freedom of expression and peaceful assembly.⁹⁵ Moreover, FRT has emerged as a powerful tool posing serious privacy risks.⁹⁶ Privacy is fundamental to "dignity, autonomy, and personal growth," and it is a requirement to "free and open participation" of society's members in a democracy.⁹⁷ Hence, when surveillance increases, individuals can be

⁹⁰ *Ibid* at para 121.

⁹¹ *Ibid* at para 3.

⁹² *Ibid*.

⁹³ *Ibid* at para 4.

⁹⁴ Daniel Therrien, "Police Use of Facial Recognition Technology in Canada and the Way Forward" (10 June 2021), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/> [perma.cc/9PCM-EJ49] [Police Use of FRT].

⁹⁵ *Ibid*.

⁹⁶ Office of the Privacy Commission of Canada, "Privacy Guidance on Facial Recognition for Police Agencies" (2 May 2022), online: *Office of the Privacy Commissioner of Canada* <priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/> [perma.cc/3WYK-CHRA] [Guidance on FR].

⁹⁷ *Ibid* at para 12.

deterred from meaningfully exercising their rights and freedoms.⁹⁸ Additionally, the Commissioner points out that:

The freedom to live and develop free from surveillance is a fundamental human right. In Canada, public sector statutory rights to privacy are recognized as quasi-constitutional in nature, and aspects of the right to privacy are protected by sections 7 and 8 of the *Canadian Charter of Rights and Freedoms* (the Charter). These rights dictate that individuals must be able to navigate public, semi-public, and private spaces without the risk of their activities being routinely identified, tracked and monitored.⁹⁹

Thus, what exactly is facial recognition (“FR”) and how does it work? The Office of the Privacy Commissioner of Canada describes the use of FR as involving:

... the collection and processing of sensitive personal information: biometric facial data is unique to each individual, unlikely to vary significantly over periods of time, and difficult to change in its underlying features. This information speaks to the very core of individual identity, and its collection and use by police supports the ability to identify and potentially surveil individuals.¹⁰⁰

More specifically:

FR technology is a type of software that uses complex image processing techniques to detect and analyze the biometric features of an individual’s face for the purposes of identification or verification (also known as “authentication”) of an individual’s identity. While early versions relied on humans to manually select and measure the landmarks of an individual’s face, today the process of creating a facial template or “faceprint” is fully automated. Using advanced, “deep learning” algorithms trained on millions of examples, FR technology is able to create three-dimensional faceprints consisting of close to a hundred biometric features from two-dimensional images.¹⁰¹

Hence, the fact that there is no specific and stringent legal framework governing the scope of FR use in Canada is alarming. The current legal framework consists of a “patchwork of statutes and the common law,” more specifically, federal and provincial privacy laws, “statutes regulating police powers and activities and *Charter* jurisprudence.”¹⁰² Hence, Canada’s federal, provincial, and territorial privacy commissioners are of the opinion that the current legislative context for police use of FR is “insufficient” and

⁹⁸ *Ibid.*

⁹⁹ *Ibid* at para 11.

¹⁰⁰ *Ibid* at para 8.

¹⁰¹ *Ibid* at para 19.

¹⁰² *Ibid* at para 41.

“there remains significant uncertainty about the circumstances in which FR use by police is lawful.”¹⁰³

Based on the results from the previously commenced investigation on the RCMP’s use of Clearview’s FRT in February 2021, the Privacy Commissioner of Canada pointed out that “billions of people essentially found themselves in a “24/7” police line-up.”¹⁰⁴ When the RCMP collected personal information from Clearview, it contravened the *Privacy Act* because, as a government institution, the police cannot collect personal data from a third party if that third party initially collected the information unlawfully.¹⁰⁵ Erroneously, when the RCMP was initially asked by the joint investigating Privacy Commissioners whether it was using Clearview’s services, it denied it. Later, it admitted to using it but only for limited purposes, such as identifying and rescuing children who are victims of online sexual abuse.¹⁰⁶ Moreover, the Commissioner pointed out that the RCMP “has serious and systemic gaps in its policies and systems to track, identify, assess and control novel collections of personal information. Such system checks are critical to ensuring that the RCMP complies with the law when it uses new technology such as FRT, and new sources, such as private databases.”¹⁰⁷

Although the RCMP is no longer using Clearview’s services, the Commissioner remains concerned with the fact that the RCMP did not agree with the findings of the investigation and tried to defend itself by arguing that s. 4 of the *Privacy Act* does not impose a duty on the RCMP to confirm the legality of the collected personal information it obtains from the third-party vendor (Clearview).¹⁰⁸ Despite this, the Commissioner acknowledged the RCMP’s effort in launching a National Technology Onboarding Program unit in March 2021 and its commitment to implementing the recommendations made by the Commissioner.¹⁰⁹ These recommendations can be summarized as follows: the police need specific reasons based on evidence to justify the use of FRT, as well as adhere to the

¹⁰³ *Ibid* at para 2.

¹⁰⁴ Police Use of FRT, *supra* note 94, Overview of Investigation into RCMP’s use of Clearview AI.

¹⁰⁵ *Ibid*.

¹⁰⁶ *Ibid*.

¹⁰⁷ *Ibid* [emphasis added].

¹⁰⁸ *Ibid*.

¹⁰⁹ *Ibid*.

critical principles of accuracy, data minimization, accountability, and transparency prior to FRT use.¹¹⁰

The Commissioner points out that when considering the use of FR technology, police agencies must not only ensure they have a lawful authority for the proposed use, but they must also apply standards of privacy protection proportionately to the potential harms involved.¹¹¹ Police agencies must have the legal authority to use FR and use it in a manner that respects the privacy rights of Canadians.¹¹² Furthermore, the collection of personal information must be limited to what is directly relevant and necessary “for the specific objectives of an FR initiative.”¹¹³ The Privacy Commissioner of Canada strongly recommends personal information be protected “by appropriate security measures relative to the sensitivity of the information.”¹¹⁴ To stress the significance of police’s work and the inherent balance it must strike with individual human rights and constitutionally protected rights and liberties, the Commissioner states that “[p]olice agencies have a crucial role in furthering public interests such as the preservation of peace, the prevention of crimes, and the administration of justice. The common law, like statutory authorities, can authorize police actions that infringe on individual liberties in the pursuit of these societal goals.”¹¹⁵ To achieve that necessary balance, The Commissioner mandates open public access to the formal FR agency’s policy setting out the circumstances in which the agency will and will not engage in FR use and how personal information will be handled.¹¹⁶

Next, as addressed by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (“ETHI”) meeting in August 2022, the RCMP has also admitted to its use of spyware – on-device investigative tools (“ODITs”) hacking cellphones.¹¹⁷ Spyware intrudes on mobile devices and collects personal data. It also has the capacity to remotely turn on and off the microphone and cameras of a suspect’s phone or

¹¹⁰ *Ibid.*

¹¹¹ Guidance on FR, *supra* note 96 at para 34.

¹¹² *Ibid* at para 37.

¹¹³ *Ibid* at para 103.

¹¹⁴ *Ibid* at para 121.

¹¹⁵ *Ibid* at para 46.

¹¹⁶ *Ibid* at para 128.

¹¹⁷ House of Commons, *The RCMP & Spyware: A Privacy Predicament of Profound Proportions*, Privacy and Ethics (ETHI), 44-1, No 32 (09 August 2022) at 15 [ETHI].

laptop.¹¹⁸ The RCMP has done so since 2017 without even preparing a PIA.¹¹⁹ Although not mandatory, PIAs are recommended by Privacy Commissioners, and as previously discussed in Part II, they are prepared by various police agencies across Canada prior to launching new procedures involving the implementation of technology, such as BWCs. Unfortunately, the Commissioner “cannot compel any department to produce a PIA, and has no authority to sanction any department or agency for failing to prepare a PIA.”¹²⁰ Hence, as ETHI states, “allowing police to police themselves offers little in the way of genuine transparency, and that is inadequate in a democracy that relies on transparency to foster trust in government, the public sector, and the judicial system.”¹²¹ Additionally, ETHI states that police operational independence is important, but without being effectively overseen “it easily leads to policing in the shadows.”¹²²

To demonstrate how the privacy concerns surrounding subjecting BWCs videos to FRT play out in practice, a comparison of FRT and Automated License Plate Reader (“ALPR”) technology will be helpful. ALPR is a camera installed at intersections or in police patrol cars with built-in technology, allowing it to photograph license plates of passing vehicles in its frame and screen them against police internal database lists for vehicles linked to crimes.¹²³ With the help of ALPR, police is able to track the movements of the vehicle throughout the city and create a “pervasive account of a car’s location.”¹²⁴ While it is public knowledge that ALPR and FRT exist, the specific methods of their use and deployment are not disclosed and may be “invisible” even to “oversight institutions.”¹²⁵ In the eyes of the courts, the use of ALPR does not constitute a search; hence the accused persons are unable to exclude evidence obtained with the assistance of ALPR.¹²⁶ Furthermore, drivers may never know they are being tracked

¹¹⁸ *Ibid.*

¹¹⁹ *Ibid* at 14–15.

¹²⁰ *Ibid* at 14.

¹²¹ *Ibid* at 3.

¹²² *Ibid.*

¹²³ Hannah Bloch-Wehba, “Visible Policing: Technology, Transparency, and Democratic Control” (2021) 109 Cal L Rev 917 at 919.

¹²⁴ *Ibid.*

¹²⁵ *Ibid* at 920.

¹²⁶ *Ibid.*

unless they are charged with a crime and ALPR evidence is disclosed.¹²⁷ These same principles and concerns apply to the police's use of FRT. Hence, as Hannah Bloch-Wehba outlines, "law enforcement techniques that rely on advanced technologies are often less visible to individual targets, the judicial branch, and the public than their physical counterparts."¹²⁸ Moreover, there is mixed evidence about the accuracy of FRT and the "high potential cost of error" it sometimes generates.¹²⁹ FRT misidentifies people of colour more frequently as potential matches than Caucasian faces.¹³⁰ Such errors lead to the perpetuation of differential treatment of people of colour and discriminatory practices of authorities – the exact opposites of the values of transparency and accountability BWCs are meant to promote. Coupled with the ability to covertly track an individual's movements across town, BWCs footage subjected to FRT could easily turn into a police tool of total control over the individual and not only violate one's privacy but also disregard an individual's liberties.

To sum up, knowing about the RCMP's infractions with privacy laws and its tendency to unilaterally employ recent technology and practices into its operations with little or no regard to how an individual's privacy may be negatively affected or entirely compromised, Canadian society and Privacy Commissioners across various jurisdictions must be vigilant about the RCMP's BWCs implementation project. Although their BWCs policy explicitly states that BWCs data will not be subject to FRT, there is no guarantee that the RCMP will not covertly subject the data to FRT or that the vendor company contracted to supply and maintain their software and the DEMS will not misuse the gathered information similarly to how Clearview did. Moreover, the fact that the RCMPs BWCs are constantly recording elevates the concern that large amounts of data lacking third-party consent is being gathered and easily abused or exploited for alternative gains. Equivalent concerns about the use of FRT of BWCs footage and the misuse of digital data captured via BWCs apply to other police agencies across the country.

Conversely, the RCMP's BWCs rollout could lead to more unified, streamlined, transparent, accountable, and progressive policing in Canada if properly implemented and maintained. As discussed, the current

¹²⁷ *Ibid* at 320.

¹²⁸ *Ibid* at 921.

¹²⁹ *Ibid* at 956.

¹³⁰ *Ibid* at 956–957.

statutory framework has gaps in privacy protection and in holding police responsible for their wrongdoings where privacy infractions ensue. Nevertheless, laws are not static but evolve as society progresses. Therefore, there is the possibility to develop an effective legal framework to capture these new advancements in policing and ensure the safe employment of technology with sufficient planning and collaboration across all levels of government.

CASE STUDIES: THE USEFULNESS AND FLEXIBILITY OF BWC PRODUCED DATA AS EVIDENCE IN COURT PROCEEDINGS

The most effective way to illustrate the usefulness and advantages of evidence obtained via BWCs is through real-life examples. What follows is an overview of eight criminal cases from the jurisdiction of Calgary, Alberta, demonstrating the reliability and flexibility of evidence obtained via BWCs. Calgary is currently the only large urban municipality in the prairie provinces that has invested in and fully equipped its front-line officers with BWCs. The cases are selected based on various legal issues before the court, including the analysis of Charter rights. In addition, there are numerous different settings and circumstances in the cases showcasing the assistance BWCs footage can provide not only to police officers on the scene of an incident but also to Crown prosecutors, defence counsels, accused persons, judges, juries, and other players within the criminal justice system.

A. R v Saunders¹³¹

R v Saunders is a case involving drug trafficking charges and a *Charter* *voir dire*. The accused had been under police observation for some time before a search warrant for the search of his apartment was granted. An unmarked police vehicle was asked to follow Mr. Saunders while driving on a highway and conduct an arrest of him. Interestingly, one of the arresting officers did not know that his BWC was already activated as soon as Mr. Saunders was directed to pull his vehicle over. The officer noticed that his camera was on after the interaction concluded, and the accused was being transported to the arrest processing unit. The same officer exercised excessive force and hit the accused before informing him about the reasons

¹³¹ *R v Saunders*, 2021 ABPC 77 [*Saunders*].

for the pullover and the arrest. Also, the BWCs captured how the other arresting officer proceeded to search Mr. Saunders' cell phone for information that might assist the ongoing investigation without having formal authorization to do so.

The defence brought an application for violation of Mr. Saunders' sections 7, 8, 9, 10, and 11(d) *Charter* rights and sought a section 24(2) *Charter* remedy. The court found that sections 7, 8, 10 (a), and 10(b) were violated and excluded from trial the drugs obtained from the search of Mr. Saunders's apartment. This finding was possible because of the captured interaction between Mr. Saunders and the arresting officers on their BWCs and the amount of undisputable detailed evidence it provided to the judge in favour of most of the alleged *Charter* violations. Hence, the BWCs footage assisted the court in substantiating the judge's decision and in providing details for the application of corresponding legal tests, which are highly context specific. The presiding judge was able to see and hear the interaction between the arresting officers and the accused, the language used by the officers, and the amount of force exerted unnecessarily over the accused, as opposed to simply reading a police report and hearing the one-sided statements of the officers backed up by their written notes when questioned on the witness stand. Additionally, it is important to note that the values of accountability and transparency were upheld through the production of the footage as part of the disclosure to the Crown. Even though the BWCs evidence did not support the Crown's case, the system is working properly, as it should, by neutrally disclosing that evidence and allowing the trier of fact to make their determination about its weight and the outcome of the case.

B. *R v Henderson*¹³²

This case outlines a blended *voir dire* hearing and is an example of the escalation of charges as the interaction between officer-citizen develops in instances of a car accident. Ms. Henderson was the driver of a vehicle involved in a car crash. Initially, the responding officer did not suspect that alcohol was involved. As the responding officer approached Ms. Henderson closely while handing her the paperwork for the incident, he smelled alcohol coming from her direction. However, the officer was uncertain whether the smell of alcohol came from Ms. Henderson. Ms. Henderson

¹³² *R v Henderson*, 2020 ABPC 60 [*Henderson*].

also exhibited strange behavior as she kept turning away from the officer while speaking with him. This raised his suspicion, and he proceeded with an ASD demand. The result from the ASD test substantiated the need for a breath demand.¹³³ The officer advised Ms. Henderson of her right to counsel pursuant to section 10(b) of the *Charter* and cautioned her. At the police station, the officer provided Ms. Henderson with the phone number for legal aid and the phonebook where she could locate phone numbers for other lawyers.

Then, Ms. Henderson sought to exclude the breath sample she provided at the police station, alleging that her sections 8, 10(a), and 10(b) *Charter* rights had been violated. Because the entire interaction between Ms. Henderson and the arresting officer was recorded on his BWC, the court was able to see Ms. Henderson acknowledging that she understood her caution and right to counsel with her boyfriend at the scene. The BWC also captured the interaction between Ms. Henderson and the arresting officer at the police station when she was provided the opportunity to contact legal counsel. Additionally, the BWC video and its built-in date and time feature assisted the court in applying the “as soon as practicable” test and the “reasonable suspicion” test. Time is of the essence for impaired driving charges because there is a limited window to obtain a proper breath sample.

This case demonstrates that relying only on the BWC footage might lead to misleading information provided to the court, which is why it is important to always have the *viva voce* evidence of (ideally) the officer, who was wearing the BWC, who can articulate the contextual meaning of his words in the totality of the situation captured on the BWC. Therefore, BWCs videos and images should not replace the officer’s written notes and oral testimony but complement them. In conclusion, the court found no breach of Ms. Henderson’s *Charter* rights, and the Certificate of Analysis of her breath sample was admitted into evidence.

C. R v Daytec¹³⁴

R v Daytec is another driving while intoxicated case, which also has a charge of failing without reasonable excuse to comply with a proper demand for a breath sample. Video footage obtained from the police cruiser and the BWCs of the involved officers exhibited to the court the irregular driving

¹³³ *Ibid* at para 14.

¹³⁴ *R v Daytec*, 2021 ABPC 48 [*Daytec*].

pattern of Mr. Daytec, as well as his appearance (reading glasses were sideways) and behaviour when he was pulled over. The entire interaction between the accused and police officers was recorded on BWCs and provided to the Crown. Mr. Daytec testified at his trial that he was confused about the directions one of the officers was providing him with regarding how to blow into the breathalyzer. Hence, Mr. Daytec was unable to provide a proper second breath sample, which resulted in his additional criminal charge.

Based on the BWC video played in court, the defence counsel was able to pinpoint flaws in the officer's instructions and those provided as per the device's manual. Defence counsel also pointed out that the manual prescribes three sets of three breath sample attempts, while the officer only allowed Mr. Daytec seven attempts; hence depriving him of two more tries. Notably, the BWC video demonstrated a power dynamic between the officer trained to use the device and another officer nearby, who, without proper training on the operation of the breathalyzer, interfered with Mr. Daytec. The court deemed improper the interference of the untrained officer with the breath sample of Mr. Daytec. Hence, the court found Mr. Daytec not guilty on the charge of failing without reasonable excuse to comply with a proper demand for a breath sample and guilty of the driving while intoxicated charge. To sum up, BWCs footage can help accused persons achieve just verdicts by having solid evidence in their defence as opposed to relying on the court to assess the weight of accused vs. officer oral testimony. Also, BWCs provide undisputable evidence about driving patterns, appearances of the accused, and other contextual factors assisting decision-makers in their deliberation and weighing of facts.

D. R v Saddleback¹³⁵

R v Saddleback is a domestic violence case involving sexual assault, assault, assault with a weapon, unlawful confinement, and threat to cause death or bodily harm charges. It demonstrates the struggle the police and courts face when dealing with domestic violence cases. Often, there are inconsistencies in the victim's statements at the time of the incident and later in court, which is utilized by defence counsel as a means to undermine the victim's credibility and persuade the trier of fact to draw negative inferences about the victim. The BWCs videos from the officers responding

¹³⁵ *R v Saddleback*, 2020 ABPC 168 [*Saddleback*].

on the scene provided fresh evidence of the statements and behaviour of the victim at the time of the incident. In that sense, the BWCs were used to substantiate and perpetuate defence's methods of questioning and undermining the victim's credibility. However, the issue here is not with the BWC evidence or its quality but the way it is used. In addition, there was missing physical evidence alleged to have been used in the commission of some of the alleged offences (duct tape and metal bar), which further undermined the victim's credibility. In this case, BWCs were also used to capture the injuries of the victim at the time of the incident. However, it is important to note that bruises may take up to several days to appear on the skin, and, in this regard, BWCs images may be improperly relied on as evidence of bodily injuries at the time of incidents. In the end, due to the inconsistencies in the victim's testimony, the accused was only convicted on two of the charges faced by him— assault and sexual assault.

E. *R v YK*¹³⁶

R v YK was another domestic violence case involving serious aggravated assault and strangulating charges. The victim refused to testify in court, although she was subpoenaed. At *voir dire*, the BWCs footages from the officers responding to the incident at the time it occurred was the only piece of evidence that could be presented in court, and it was tested under both traditional and principled approaches of the hearsay evidence rules. The BWCs videos were divided into three parts, and only part one captured the victim and her statements immediately after the incident was admitted into evidence. There was a high degree of detail about the victim's statements and appearance at the time, which may be easily missed or omitted in the officer's written notes. Likewise, the change in the victim's behaviour in the ambulance can best be demonstrated through video footage vs. written notes. The flexibility and reliability of BWCs footage are evident here again. Moreover, its usefulness to the Crown in determining the likelihood of conviction and guarding the public interest in the pursuit of justice and community safety is undeniable. Had there been no video evidence obtained via BWCs, the case would likely have proceeded without the key witness.

¹³⁶ *R v YK*, 2019 ABPC 249 [YK].

F. *R v Chernoff*¹³⁷

R v Chernoff was a sentencing case regarding criminal charges arising from a domestic incident with mischief and damage to property charges. The parties had already agreed to the facts. The judge relied on the BWC video of a responding officer to account for details regarding the remorse and admission of guilt by the accused after his arrest and while he was transported to the hospital. The entire officer-accused interaction was captured on the BWC of the officer, and it showed the behaviour of the accused that led to the deployment of a taser and his subsequent arrest. The exact moments of deploying the taser, cautioning, and arresting the accused were time stamped because of the BWC capabilities. Also, it was easy for the judge to see the condition of the home and the extent of property damages inflicted on the victim. In addition, the BWC recorded the officer serving the accused with an Emergency Protection Order (EPO) the following morning as he was released from the hospital. BWC video can easily verify the service of the EPO with certainty and eliminate the possibility of the respondent claiming that (s)he was never served and did not know about the existence of it, which is common.

G. *R v Wol*¹³⁸

In *R v Wol*, two co-accused were charged with unlawful possession of a prohibited or restricted weapon and breaking and entering a dwelling home with the intent to commit an indictable offence. Witnesses' testimony was inconclusive and discredited by the defence counsel at cross-examination. The identity of one of the co-accused was also at issue before the court. The piece of evidence that helped the judge to identify the two co-accused and conclude beyond a reasonable doubt that they owned a prohibited or a restricted firearm was an exhibit with a still image of both co-accused in an SUV outside the home as they were trying to drive off upon police's arrival. This image was captured by the BWC of one of the officers responding to the incident. Notably, the judge stated that "[t]hese photographs coupled with the evidence of Cst. Harris lead me to the conclusion that Mr. Wol had possession of the sawed-off shotgun at the time it was discharged."¹³⁹ This illustrates one of the multiple useful features of BWCs and their ability

¹³⁷ *R v Chernoff*, 2021 ABPC 16 [*Chernoff*].

¹³⁸ *R v Wol*, 2019 ABPC 304 [*Wol*].

¹³⁹ *Ibid* at para 55.

to transform videos into clear images. If Cst. Harris had not worn a BWC, or if his BWC had been turned off, it would have been very difficult, if not impossible, for the Crown to meet its burden of proof beyond a reasonable doubt in identifying one of the co-accused. Moreover, because the BWC footage transformed into a clear image of the co-accused together in the SUV and Mr. Wol holding the firearm while his hands were in the air, the court was also able to convict the co-accused of possession of a firearm and a subsequent count of breaching previous court orders, since there were weapons and firearm prohibition orders in effect.

H. *R v Callaghan*¹⁴⁰

R v Callaghan involves an accused being pulled over for driving while intoxicated just as he was parking at the driveway of his home. One of the issues raised by the defence counsel at the blended *voir dire* was that the Crown had failed to identify the accused properly. The police officer who conducted the arrest testified as one of the witnesses at trial and identified the accused at the dock based primarily on his interaction at the time of the arrest and at the subsequent serving of court documents, including a Promise to Appear. The interactions between the arresting officer and the accused were recorded on the BWC of the arresting officer and were relied upon at trial. The judge regarded the BWC video as highly reliable, good quality, and detailed evidence, which helped reveal the physical appearance of the accused – body type, height, facial features, and visible tattoos – and assisted the judge in refuting the arguments raised by the defence counsel. The judge found that the accused in the courtroom is the same person depicted on the BWC and is the person who should hence be charged with the offence of driving while intoxicated. Although not applicable in this case since the accused refused to testify, BWC videos also record high-quality sound. Therefore, the voice of the accused is another unique characteristic that could help identify the accused before the court. However, the issue is that the Canadian justice system does not require the accused to testify at their trial. Hence, maybe a change is needed for a new approach or a legal rule requiring the accused to read a neutral script (as opposed to answering questions asked on the stand), which can help the judge and jury identify him. This will be another step towards better

¹⁴⁰ *R v Callaghan*, 2020 ABPC 208 [Callaghan].

utilization of the features of BWCs. This will also help the Crown to meet its onerous burden of proof beyond a reasonable doubt.

I. Summary of features and usefulness of evidence obtained via BWCs

As illustrated through the eight preceding cases, evidence produced by BWCs is objective, reliable, and has numerous practical applications in the criminal justice system. For example, as seen in *Saunders*, it can assist the accused in proving alleged *Charter* violations by arresting officers and use of violence and excessive force. The fact that the trial judge noted the officer's misconduct proves that BWCs enhance trust and transparency in the police and can be utilized as accountability tools for police conduct. Furthermore, BWCs provide clear timelines and time stamps of the officer's interactions with an individual and capture the language used and the context in which certain words are used so that a trier of fact has a complete picture of the accident and the interaction in question. Therefore, BWCs easily prove the timeliness of police caution, instructions, and reading of *Charter* rights. However, as seen in *Henderson*, relying only on BWCs footage should be avoided, and officers' notes and court testimony must be considered in conjunction with the digital evidence. Next, BWCs footage can demonstrate a person's driving patterns and appearance in cases involving impaired driving, as shown in *Daytec*. In addition, the same case illustrated how BWC footage assisted the defence counsel in pinpointing gaps in the officer's training in providing instructions to the accused on how to submit a proper breathalyzer test. This resulted in an acquittal for the accused on one of his charges.

Unfortunately, as illustrated in *Saddleback*, BWCs are used as tools to undermine victims' credibility in sexual assault cases. It is important to note, however, that the issue is not with the technology or the quality of the evidence produced by the BWCs, but in the way the system applies and turns it against the victims by hinging on inconsistencies in their testimony provided immediately after the alleged incident and later in court. Moreover, in assault and domestic violence cases, BWCs are useful for capturing injuries, but it is crucial to note that bruises may take several days to become visible, so one should not rely solely on the BWCs footage and images generated from them. Also, in domestic violence cases when the victim, which is often the main Crown witness, refuses to testify in court (usually out of fear), BWCs footage is extremely helpful evidence for the

court and for the Crown prosecutor, who can proceed with the case in the public interest even without the victim's court testimony. These were the circumstances in *Y.K.* Likewise, evidence produced by BWCs in the domestic violence context is also useful for capturing the extent of property damages as seen in *Chernoff* and proving service of an EPO upon the respondent. Also, since the same case required the officer's deployment of a taser, the entire interaction between the officer and the accused was captured, which provides insurance for both the officer and the accused should the events escalate or if complaints against the officer are filed.

Wol demonstrated the use of BWCs footage to prove the identity of the accused and his ownership of a firearm at the time of the incident while subject to an active firearm prohibition order. Lastly, *Callaghan* reiterated the usefulness of BWCs in proving the identity of the accused in court in very different circumstances than in *Wol*, and it left the door open for a potential evolution of court proceedings, where the voice of a suspect can be authenticated with the use of a BWC recording. *Callaghan* is also an example of the transparent and unbiased police and criminal justice system, where regardless of the status of the accused as an off-duty police officer, he was charged with driving a motor vehicle while intoxicated by his colleague.

DIGITAL DATA, POLICE MISCONDUCT IN PUBLIC OFFICE, AND UPHOLDING THE RULE OF LAW

*A. R v Collins; R v Lewis and Jaffer*¹⁴¹

In May 2022, the Court of Appeal (Criminal Division) in London, Britain, refused to grant leave to appeals regarding the sentencing of two police officers and one civilian police staff member found guilty of misconduct in public office for the creation, possession, and misuse of crime scene photographs. A Canadian scholar states that as a highly regulated profession, police officers should be held accountable to the same high standards applicable to other highly regulated professions, such as the legal profession, in ensuring public trust and confidence.¹⁴² Furthermore, the court highlighted that civilian police staff must also be held accountable to the same standards police officers are. Collins worked as a Digital

¹⁴¹ *R v Collins; R v Lewis and Jaffer*, [2022] EWCA Crim 742 [Collins].

¹⁴² Tale of the Tape, *supra* note 87 at 292.

Forensics Expert and transferred thousands of crime scene and murder victims' images onto a flash drive and subsequently to his personal computer. He did not disseminate the images any further. He was sentenced to three years in prison. Lewis and Jaffar were two police officers assigned to preserve the integrity of a crime scene where two women had been murdered in a public park, and their bodies remained at the scene. Both officers failed to continuously secure access to the scene, as they left their assigned posts and took images of the crime scene, including of the dead bodies, which they disseminated with social media friends. They might have also easily contaminated the crime scene and negatively interfered with the investigation and the gathering of DNA. Their actions handed leverage to the defence counsel in making an argument in favour of his client, alleging that the contamination of the crime scene may have interfered with the results of the DNA obtained. Luckily, the jury still found the accused guilty, but depending on the circumstances, this may have had a different unjust outcome. Both accused were sentenced to two years and nine months in jail.

The court pointed out the importance of the work police do, the need for public confidence in it, and the principle of upholding the rule of law. The following paragraphs directly quoted from the case capture the essence and interplay of those issues within the day-to-day police operations and society at large. While this case does not involve a direct discussion on the topic of BWCs use in these circumstances, it demonstrates the vulnerability of digital data gathered and stored by police depicting highly sensitive personal information and its easy manipulation and dissemination. Furthermore, the below-outlined principles and values are equally applicable in Canada.

[9] . . . It is essential that the public should be able to trust the police to play their proper part in ensuring that those who commit crimes are brought to justice. Conversely, the rule of law means that those who are not guilty of crimes should have the opportunity to exculpate themselves. Misconduct that undermines public trust in the process of bringing those guilty of serious offences to justice, or the process of preventing innocent people from early exculpation, must be punished severely.

[10] The retrieval, examination and storage of data in electronic formats has become essential to the investigation and prosecution of crime. Whether in the form of text or images, the collection and storage of data is an essential tool of contemporary policing and is now fundamental to the administration of justice. As the case of Collins demonstrates, electronic databases may hold vast amounts of personal and sensitive material. Those who work for the police may be entrusted with privileged access to large amounts of data that may touch on the personal

lives of victims, suspects and members of the public alike. In *R v Kassim* [2005] EWCA Crim 1020, [2006] 1 Cr. App. R. (S.) 4, para 19, this court (Lord Justice Rose VP, Bodey and Owen JJ) held:

“It seems to us that, especially nowadays, the preservation of the integrity of information regarding members of the public held on databases like those maintained by the police is of fundamental importance to the well-being of society. Any abuse of that integrity by officials including the police is a gross breach of trust, which, unless the wrongdoing is really minimal... will necessarily be met by a severe punishment, even in the face of substantial personal mitigation.”

[11] If data is copied or disseminated other than in lawful ways for lawful purposes, it carries the inevitable risk that neither the police nor the victims of crime nor their families will be able to control who sees it or the circumstances in which it is viewed. In the cases before us, the statements that we have read from family members movingly describe the deep distress caused by their loss of control of the treatment of those for whom they grieve.

[12] The harmful effects of the misuse of electronic images may be impossible to rectify. The ease with which images may be disseminated by electronic means (via phones, laptops and other devices) and the difficulty in controlling their spread is an important aspect of the harm caused by offences of this kind.¹⁴³

B. Police Misconduct in Public Office in Canada

In Canada, there has been a recent case of an internal breach of highly sensitive information. In September 2019, Mr. Cameron Ortis, the Director General of the RCMP's National Intelligence Coordination Center (a civilian position), was charged with a number of offences under the *Security of Information Act* and the *Criminal Code*.¹⁴⁴ Between January 01, 2014, and September 12, 2019, Mr. Ortis leaked information to foreign entities for allegedly personal gain and compromised national security and Canadian international relations.¹⁴⁵ His trial, initially scheduled for September 2022, has now been postponed for a year due to a change in his defence counsel.¹⁴⁶ Due to the sensitive nature of the proceedings surrounding this high-profile case, a Federal Court order is in place that prohibits the publication or broadcasting of the evidence that the Public Prosecution Service of Canada

¹⁴³ *Collins*, *supra* note 141 at paras 9–12.

¹⁴⁴ *Canada (Attorney General) v Ortis*, 2021 FC 737 at paras 1, 12 and 13.

¹⁴⁵ The Fifth Estate, “The Smartest Guy in the Room” (2021), online (video): *YouTube* <www.youtube.com/watch?v=2ni9c23aHDA&t=468s> [perma.cc/6CPZ-P9FV].

¹⁴⁶ The Canadian Press, “Trial of RCMP Employee Accused of Leaking Secrets Delayed by 1 year” (1 September 2022), online: *Global News* <globalnews.ca/news/9099504/rcmp-secrets-leak-trial-delayed/> [perma.cc/Y2NL-L2GH].

will present in the criminal trial pursuant to section 38.04 of the *Canada Evidence Act*.

This example, although again not directly involved with BWCs, illustrates the importance of proper safeguard measures built within the RCMP and other police forces so that access to digital information is highly restricted and frequently monitored. Digital data could be easily abused and mismanaged if placed in the hands of a malicious handler. Therefore, since BWCs produce a high volume of sensitive personal information in the form of digital data, the strictest measures of its collection, storage, access, archiving, and reproduction must be enforced. In addition, cases involving police or civilian police staff misconduct must be publicized, and accused persons found guilty of police misconduct in public office must be subject to severe penalties and lengthy sentences. Furthermore, as discussed in Part III of the paper, the current legal framework navigating police agencies' relationships with third-party vendors supplying and maintaining software and hardware for digital data gathering and storing must be strengthened so that incidents like the one with the RCMP and Clearview do not reoccur. If they do, there must be serious consequences for the police and the company. Consequently, all these measures must be in place for the Canadian criminal justice system to demonstrate to the public the seriousness of such misconduct and to uphold the principles of transparency, accountability, and applicability of the rule of law.

NOW AND THE PROPOSED PATH FORWARD

The themes discussed in this paper reveal two major contradicting principles surrounding the police's use of BWCs. On the one hand, they can be very useful for evidence-gathering purposes and assist various players within the criminal justice system. For example, BWCs videos can often be the only effective tool providing members of the public with grounds to raise their voices and protect their *Charter* rights from infringements, especially in cases of alleged officers' use of abuse of authority or excessive force.¹⁴⁷ BWCs are regarded as means of improving officer-citizen relationships by enhancing the public's trust in the police. On the other hand, the digital data gathered via BWCs are highly sensitive, in large quantities, and easily manipulated and abused. Privacy is a serious concern

¹⁴⁷ See *Saunders*, *supra* note 131.

in connection with managing the electronic recordings and images gathered via BWCs. As discussed in Parts II and IV, Canada, and the RCMP specifically, has recently experienced breaches of privacy and currently lacks effective preventative measures for addressing and preventing such breaches. Hence, there must be strict internal and external measures guarding DEMS and the manipulation of data obtained via BWCs, to protect the privacy of the individuals and the public depicted in those recordings or images. Furthermore, BWCs gathered data should not be subjected to FRT unless strictly regulated by an external governing body. Cases of misconduct should be publicized to demonstrate the seriousness of police misconduct and promote accountability and transparency in the public eye. The use of BWCs across Canada is scattered and lacks uniformity. Some police agencies have more “robust” BWCs policies than others.¹⁴⁸ Currently, in Canada, BWCs are mainly implemented in a few large cities – i.e., Vancouver, Calgary, and Toronto. This year, the RCMP will be adopting the use of BWCs in all their front-line operations and locations. This means that rural and remote areas of Canada will now enjoy the benefits of this technology, and so will local courts along with corresponding players in the justice system. Although speculative, the impact of such vast changes must be considered. As demonstrated, the use and value of BWCs-generated digital evidence in court are immense. Therefore, only some judges, Crowns, and juries in parts of the same province will be able to enjoy the benefits of that digital evidence and make more substantiated decisions, while others will not.

In addition, this lack of uniformity and availability of BWCs in each part of the same province may create tension between the RCMP and other police agencies. Moreover, different practices and technological features of the BWCs and DEMS and their corresponding policies and procedures will also contribute to various standards of policing across jurisdictions. For example, some jurisdictions allow officers to have access to the BWC video and/or can take notes within the digital recording, as well as augment their written notes with details upon viewing the BWC footage. Inevitably, a serious consideration of such practices must be given in the context of their potential impact on the Crown prosecutor’s perception of the case when assessing the evidence before them. Since Crown prosecutors must evaluate the strength of the evidence and determine whether, on a balance of

¹⁴⁸ Tale of the Tape, *supra* note 87 at 249.

probabilities, there is a likelihood of conviction, having officer's notes within the BWC footage may impact that evaluation and decision-making. Therefore, standard practices of submitting BWC footage to Crown prosecutors without embedded officer notes should be adopted across all jurisdictions to ensure consistency and impartiality.

As previously discussed, each police agency relies on its external third-party vendor for the service provision, storage, and maintenance of the electronic data gathered via BWCs. Hence, as the Clearview example demonstrates, there are multiple risks associated with contracting those third-party vendors - often foreign companies. The safest alternative is to be self-sustained and not have to rely on a third-party vendor, but bringing the digital infrastructure of all police agencies up to date and continuously maintaining it may be an impossible task. Hence, strictly enforced measures and obligations should be imposed on those third-party vendors when they partner with a Canadian law enforcement agency.

As demonstrated in Part III, the RCMP has a dark history regarding breaches of privacy and its lack of protective measures within its practice. Even though the RCMP's BWCs policy explicitly states that BWC video and images will not be subject to FRT, their past behaviour raises reasonable concerns, especially when coupled with the fact that there is no effective supervision over the operations of the RCMP or the rest of the police agencies in Canada by another government department. Who polices the police? This question emerges when thinking about guarding privacy and effective police operations. Privacy Commissioners only issued guidelines and recommendations for police operations, but as discussed earlier, these are not binding. Hence, nobody knows what goes on internally within police operations. Therefore, it is safe to conclude that Canada has much larger issues that exceed the questions pertaining to the use of BWCs or FRT. That issue is related to a lack of consistency and control over police forces across the nation.

Additionally, as stated in some of the reviewed BWCs policies, not only should officers and police civilian staff be trained on the proper operation of digital data, but judicial and legal training about technology and digital data should also be adopted as a national goal among Benches and Bar Associations across the country.¹⁴⁹ As discussed by ETHI:

¹⁴⁹ ETHI, *supra* note 117 at 21.

"[M]embers of the Bench and Bar who use digital devices generally do so without understanding what the technology does and can do; about how malware and spyware work; about artificial intelligence and the surveillance economy; about personal and organizational privacy and access rights and responsibilities; and about the extent and severity of harms and unintended consequences that can result from digital technologies."¹⁵⁰

Without such continuous training, judges and lawyers are left unsupported, and they must rely on their research when encountering cases with breaches of privacy issues or other issues arising from the mishandling of electronic data. Consequently, this leads to wide knowledge gaps among judges and lawyers, yielding to inconsistent levels of capable legal representation and sometimes perhaps ill-informed judicial decision-making.

If utilized well, BWCs can improve internal police operations. For example, as observed in *Daytec*, gaps in officer's training transpire through BWCs footage, and so can repeated patterns of officer misbehaviour and frequent use of force be tracked by supervisors. This may also be a sign of a training gap, an underlining issue such as PTSD, or another condition the officer may be suffering from. Hence, BWCs can provide a more proactive approach toward supporting officers' needs and minimizing instances of police use of excessive force. This requires time and resources to compile and analyze digital data to see the big picture. Unfortunately, police budgets are limited. Yet, if set as a goal, it could be achieved, and the technology allowing it exists.

Other ways of effective enjoyment of the BWC features may be the adoption of certain new practices by courts. For example, develop a new legal rule imposing a *prima facie* negative presumption against the case of the Crown in circumstances where BWCs should have been activated, but were not. Furthermore, the meaning and scope of the right against self-incrimination by testifying in court must be revisited and re-defined in light of this new technology. For instance, in cases where the defence alleges that the Crown has not proved the identity of the accused beyond a reasonable doubt, as the issue in *Callaghan* was, a judge should be allowed to request that the accused reads a neutral script, which will allow the trier of fact to hear their voice and compare it with the one recorded on the BWC.

¹⁵⁰ *Ibid.*

The province of Manitoba deserves special consideration regarding BWCs implementation. BWCs are barely used in Manitoba. Currently, Winnipeg, as the largest city and the capital of the province, does not use BWCs – not because Winnipeg Police Service (“WPS”) does not wish to implement them, but because of budget constraints preventing it from doing so.¹⁵¹ This is a great paradox, especially knowing that WPS has in its arsenal drones, four-legged robots (Spot), and K9 dog armor technology equipped with the ability to attach cameras onto it – the same technology utilized in the US in the fight against terrorism.¹⁵² Now, with the RCMP’s initiative of rolling out BWCs, another disparity will surface in terms of unequal protection of the rights of Manitobans depending on where they are located at the time of the commission of an offence. WPS is likely not the only police agency facing budgetary constraints, which is why decisions on a federal level should be made to put an end to such struggles and stop the further perpetuation of economic differences between Canadian provinces.

Based on all observations and information reviewed so far, two major propositions should be given consideration. First, the government of Canada should create a central governing body – a new institution – empowered with the task and legal capacity to effectively oversee and manage all law enforcement agencies, regardless of whether provincial or the RCMP. Let’s utilize the spirits of sections 91(27), 92(14), and 92(15) of the *Canadian Constitution Act* to their fullest potential. These central police governing body will unify BWCs policies, practices, and other differences in police operations across jurisdictions. Therefore, Canadians at each point of the country will be subject to uniform methods of protection of their *Charter* rights. Moreover, this central government body will oversee contracting with third-party vendors and secure funding for BWCs and other police operations equipment for every jurisdiction in need, like Manitoba. This body should be allowed to set aside budgets for DEMS maintenance and upgrades, which are implemented at Crown locations across Canada, to assist the justice system’s adaptation to any technological upgrades flowing from police operations. Additionally, it will also oversee

¹⁵¹ City of Winnipeg, Executive Policy Committee, “Winnipeg Police Board Budget Referral – Capital and Operating for Body Worn Cameras and Digital Evidence Management” (Council Minutes) (24 June 2021).

¹⁵² CBC News, “K9 Camera to Give Winnipeg Police New Eyes on Crime” (2013), online: CBC News <www.cbc.ca/player/play/2416566079> [perma.cc/Q7KQ-N97M].

privacy measure practices within each police department, conduct audits and ensure personal and digital information is protected to the highest available standards. Second, funding must be set aside for a Canadian study on BWCs and their effects, benefits, and the optimal utilization of their features. Collaboration among all provinces is needed to materialize such a project. Relying on foreign research is inadequate since Canada has a unique geographical and cultural landscape.

SUMMARY OF MAIN POINTS

Part II of this paper discusses the motivations behind having BWCs as part of front-line police practices and the development and use of technology in the UK and USA. Improvement of officer-citizen interactions, transparency, and accountability are the main goals behind the purpose of BWCs. As illustrated, some studies show positive outcomes with respect to achieving these goals, while others do not. Privacy concerns with the use of the technology exist, and the second sub-section of Part II discusses the approaches adopted by several Canadian police agencies prior to their implementation, as well as current policies in place for the proper use of BWCs in the field. With the mass deployment of BWCs by the RCMP this year, multiple questions and concerns arise regarding the various police practices within the same province, yielding unequal access to reliable digital evidence produced by BWCs in some jurisdictions. Consequently, Canadian *Charter* rights would be protected based on unequal substantiating evidence and standards across the country.

Part III is entirely dedicated to the topic of privacy. It outlines the more recent privacy breaches that Clearview AI – a foreign vendor contracted by the RCMP and several other Canadian police agencies providing database software and using FRT, committed by unlawfully obtaining over three billion images of Canadians from social media platforms to boost its database. Furthermore, the section describes what FRT is and how it operates. Issues such as the lack of enforceable measures of punishment to foreign vendors like Clearview AI and insufficient and inadequate legal framework governing the use of FR in Canada are also discussed. Most importantly, the RCMP's systemic gaps in its personal information gathering policies were flagged and connected with the potential dangers of BWCs generated digital data being subjected to FRT.

Part IV presents eight case studies of cases from Calgary, Alberta, illustrating the usefulness and flexibility of BWCs generated digital evidence. A summary of these BWCs evidence features and applications can be found on pages 38-39. Part V presents two British cases on the issue of police misconduct in public office by officers and civilian staff members due to their abuse and mishandling of digital data containing sensitive personal information. The decision outlines important principles of the rule of law quoted in the section. Everyone involved in these misconducts was sentenced to at least two years and nine months in prison. Following the examples from Britain, this part also presents a recent Canadian example of misconduct in public office by the former Director General of the RCMP's National Intelligence Coordination Center. While neither of these cases directly discusses BWCs generated evidence and its mishandling, the principles they establish are the focus. They demonstrate the vulnerability of digital data and its effortless manipulation and dissemination when placed in the wrong hands and not subjected to strict protective measures. Such cases must be publicized to foster transparency and accountability and enhance the public's trust in the police and other government institutions. Such wrongdoers must be subjected to severe punishments.

Finally, Part VI ties together the previously discussed topics and summarizes the two major contradicting principles associated with the use of BWCs, namely their usefulness for evidentiary purposes and means of improving officer-citizen relationships and strengthening the public's confidence in the police versus the vulnerability of digital data and the easily committed breaches of privacy. The lack of uniform police practices and measures across the provinces is discussed. The upcoming changes flowing from the RCMP's adoption of BWCs in front-line operations among the provinces broaden the gaps between these different police practices within the same jurisdiction. Consequently, propositions for further improvements are made, such as the federal designation of budget for provinces like Manitoba and other jurisdictions struggling with limited budgets preventing them from implementing the use of BWCs. Additionally, education of not only police officers and civilian staff members but also the judiciary and members of Bar Associations across the country is necessary to provide meaningful services and have substantial knowledge when tasked with cases involving digital evidence and/or privacy breach stemming from it. Evolving court proceedings could be founded upon this new technology, such as drawing negative inferences about the

Crown's case if/when a BWC should have been activated but was not. Also, the scope of the right against self-incrimination by not testifying in court should be re-defined to allow accused persons to read out loud a neutral script so that the trier of fact could compare their voice with that on a BWC recording in cases where the identity of the accused is an issue. Moreover, there is a dire need for a new government institution tasked solely with overseeing all police enforcement agencies in the country and their internal and external operations. Lastly, Canada lacks an extensive study on BWCs, and such a study should be undertaken collaboratively across jurisdictions.

CONCLUSION

BWCs are excellent tools in assisting the police in their day-to-day operations, and they strengthen the relationship between the community and the police, provide transparency and accountability, and protect *Charter* rights. BWCs assist lawyers, judges, and juries in their work and decision-making and help accused persons reach just verdicts by straightening the court record on specific details surrounding the circumstances of the offence and potential violations of their *Charter* rights. The usefulness and flexibility of BWC gathered evidence is indisputable. However, there are risks associated with the use of this technology. The largest risk is the invasion of privacy and misuse of the digital information BWCs generate. Those risks can be effectively mitigated with appropriate safety measures and vigorous supervision. There are more benefits from having BWCs than not. Hence, they should be widely implemented across all law enforcement agencies in Canada.

“Like so many other things, technology is morally neutral. How its use is justified makes the difference.”¹⁵³

¹⁵³ ETHI, *supra* note 117 at 9.