ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2023-18

May 11, 2023

PUBLIC SAFETY AND EMERGENCY SERVICES

Case File Number 005195

Office URL: www.oipc.ab.ca

Summary: The Applicant made an access request under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act) to Justice, now Public Safety and Emergency Services (the Public Body), for CCTV footage of an incident in which he had been involved at the Calgary Remand Centre on November 29, 2015. He stated:

> "Video from November 29, 2015 in regards to the brutal unsolicited assault I was subjected to at the hands of CRC staff at around 9:37 the incident has been well documented and all charge against me has been disapproved I specifically ask for the footage from the camera behind the camera that was used in my wardens court hearing as well as any other angles that may be available as well as any and all cameras that show my supposed escort to A&D. I would kindly ask for the exact times to also be provided as this is all in question as to the actual facts of the matter at hand and I would like to remove any discrepancies."

The Public Body conducted a search for responsive records. A video compiled from footage was located, but not the original CCTV footage. The Public Body withheld the video it did locate in its entirety under section 20 (disclosure harmful to law enforcement). The Public Body took the position that the video would reveal blind spots in its video surveillance system, as well as law enforcement tactics and the layout of the Calgary Remand Centre, if it were disclosed. In particular, it argued that disclosure could reasonably be expected to facilitate the escape from custody of an individual who is being lawfully detained, facilitate the commission of an unlawful act or hamper the control of crime, or harm the security of any property or system, including a building, a vehicle, a computer system or a communications system, as contemplated by section 20(1)(j), (k), and (m) of the FOIP Act.

The Adjudicator determined that it had not been established in the inquiry that disclosing the video footage the Applicant had requested would reasonably be expected to result in harms contemplated by section 20 of the FOIP Act. The Adjudicator ordered the Public Body to give the Applicant access to the video.

The Adjudicator also determined that the Public Body had not properly considered whether it was possible to sever information from the video, as required by section 6(2) of the FOIP Act.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 6, 20, 72; **BC:** *Freedom of Information and Protection of Privacy Act,* R.S.B.C. 1996, c-165, s. 15

Authorities Cited: AB: Orders F2021-42, F2022-46 **BC:** Order F08-13 **NS:** Review Report 21-04

Cases Cited: *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31; *British Columbia (Public Safety and Solicitor General) v. Stelmack*, 2011 BCSC 1244 (CanLII).

1. BACKGROUND

[para 1] The Applicant made an access request for CCTV footage of an incident in which he was involved at the Calgary Remand Centre. He stated:

> "Video from November 29, 2015 in regards to the brutal unsolicited assault I was subjected to at the hands of CRC staff at around 9:37 the incident has been well documented and all charge against me has been disapproved I specifically ask for the footage from the camera behind the camera that was used in my wardens court hearing as well as any other angles that may be available as well as any and all cameras that show my supposed escort to A&D. I would kindly ask for the exact times to also be provided as this is all in question as to the actual facts of the matter at hand and I would like to remove any discrepancies."

[para 2] A search was conducted for responsive records. A video compiled from footage was located, but not the original CCTV footage. The Public Body withheld the video it did locate in its entirety under sections 20(1)(j), 20(1)(k) and 20(1)(m) on the basis that disclosure could reasonably be expected to be harmful to law enforcement.

[para 3] The Applicant requested review of the adequacy of the Public Body's search for responsive records and its decision to withhold the video from him.

[para 4] In Order F2021-42, I ordered the Public Body to conduct a new search for responsive records and directed it to provide an account of its search to me and to the Applicant. The Public Body was unable to locate additional responsive records and provided an account of its search. It determined that the original CCTV footage had been destroyed. I reconvened the inquiry to decide the issue of the Public Body's application of section 20 to the video it did locate.

[para 5] After I reviewed the video and the submissions of the parties, I asked questions of the Public Body *in camera* so that it could provide detailed evidence and submissions regarding the information it believed would be disclosed were the requested video to be released. The Public Body provided further evidence and argument.

[para 6] I also asked the Public Body to provide me with a new copy of the video, as the video it had originally provided appeared to be missing a minute of footage. The Public Body provided a video containing the missing footage.

II. ISSUE: Did the Public Body properly apply section 20 (disclosure harmful to law enforcement)?

[para 7] Section 20 of the FOIP Act authorizes a public body to withhold information from an applicant if disclosure could be reasonably expected to result in one or more of the harms to law enforcement it enumerates. It states, in part:

> *20(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to*
>
> *[…]*
>
> *(j) facilitate the escape from custody of an individual who is being lawfully detained,*
>
> *(k) facilitate the commission of an unlawful act or hamper the control of crime,*
>
> *[…]*
>
> *(m) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system […]*
>
> *[…]*

The Public Body relies on sections 20(1)(j), (k), and (m) to withhold the video from the Applicant.

[para 8] In *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 (CanLII), the Supreme Court of Canada confirmed that when access and privacy statutes refer to reasonable expectations of harm, a party seeking to rely on the exception must demonstrate that disclosure will result in a risk of harm that is beyond the merely possible or speculative. The Court stated:

It is important to bear in mind that these phrases are simply attempts to explain or elaborate on identical statutory language. The provincial appellate courts that have not adopted the "reasonable expectation of probable harm" formulation were concerned that it suggested that the harm needed to be probable: see, e.g., *Worker Advisor*, at paras. 24-25; *Chesal v. Nova Scotia (Attorney General)*, 2003 NSCA 124 (CanLII), 219 N.S.R. (2d) 139, at para. 37. As this Court affirmed in *Merck Frosst*, the word "probable" in this formulation must be understood in the context of the rest of the phrase: there need be only a "reasonable expectation" of probable harm. The "reasonable expectation of probable harm" formulation simply "captures the need to demonstrate that disclosure will result in a risk of harm that is well beyond the merely possible or speculative, but also that it need not be proved on the balance of probabilities that disclosure will in fact result in such harm": para. 206.

Understood in this way, there is no practical difference in the standard described by the two reformulations of or elaborations on the statutory test. Given that the statutory tests are expressed in identical language in provincial and federal access to information statutes, it is preferable to have only one further elaboration of that language; *Merck Frosst*, at para. 195:

> I am not persuaded that we should change the way this test has been expressed by the Federal Courts for such an extended period of time. Such a change would also affect other provisions because similar language to that in s. 20(1)(*c*) is employed in several other exemptions under the Act, including those relating to federal-provincial affairs (s. 14), international affairs and defence (s. 15), law enforcement and investigations (s. 16), safety of individuals (s. 17), and economic interests of Canada (s. 18). In addition, as the respondent points out, the "reasonable expectation of probable harm" test has been followed with respect to a number of similarly worded provincial access to information statutes. Accordingly, the legislative interpretation of this expression is of importance both to the application of many exemptions in the federal Act and to similarly worded provisions in various provincial statutes. [Emphasis added in original.]

This Court in *Merck Frosst* adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in *Merck Frosst* emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground: paras. 197 and 199. This inquiry of course is contextual and how much evidence and the quality of evidence needed to meet this standard will ultimately depend on the nature of the issue and "inherent probabilities or improbabilities or the seriousness of the allegations or consequences": *Merck Frosst*, at para. 94, citing *F.H. v. McDougall*, 2008 SCC 53 (CanLII), [2008] 3 S.C.R. 41, at para. 40.

[para 9] Section 20 employs the phrase "could reasonably be expected to". Accordingly, the onus is on the Public Body to establish that it has a reasonable expectation that disclosure would result in harms that are probable and not merely speculative.

[para 10] The Applicant stated in a letter dated "Juneteenth" or June 19, 2020:

> This has gone on for quite some time. Years actually, the fact of the matter still remains that the Office of the Information & Privacy Commissioner **(OIPC)** was not the problem at any point for me during this very hectic and undeniably malicious ordeal that I have been in the care, custody and control of the Government of Alberta; the **STATE.** The entire purpose of me having opened this file 005195 was to receive closure and get the answers that have been-so-very elusive as to what had truly happened to me on that horrific night (November 29th 2015). Let me be frank, I was unconscious for most of what had occurred that night on the healthcare unit **(HCU)** @

Calgary Remand Center **(CRC).** It was only because of the kindness of a few separate correctional officers **(COs)** that I even knew to look further into the situation, as they had told me that I should look deeper into the incident because some *"messed up stuff happened to you and it was other CDs that did some foul things to you".*

That "tip", and the fact that I was institutionally charged 4 times **-3 were dismissed due to lack of evidence and** I **was found NOT guilty for the fourth as the video does not show the inmate being aggressive.** It is important to remember that I was in a cast as I had broken my hand 4 days prior and that was why I was on the HCU to begin with. But for those two occurrences coupled with the inexplicably malicious prosecution of myself that resulted in me further being street charged which eventually ended up being *"stayed"* by the court. I never would have gotten any CCTV footage of the incident because "they" (CRC) would just say that **disclosure of the video would** *be "harmful to law enforcement" section 20 of the FOIP act.*

[…]

This case has gone on for far too long and it has had an untold amount of negative effects on me as a person, this entire incident has been the proximate cause to the complete and absolute annihilation of my name, and life! It has also left me with permanent injuries both physically and psychologically. What had occurred was brutally vicious and incomprehensibly unconscionable misconduct by STATE ACTORS (in upper management). They obviously felt it was acceptable to alter legally binding CCTV footage […].

[…]

Unfortunately for me I had on a fairly large cast on my right hand, that I had broken 9 days prior and was told by the Doctor I would need to wear for 6 weeks. While he had tried to place these cuffs on me they didn't fit due to the big cast on my hand, at that time he had "improvised" and used the handcuffs as brass knuckles and struck me one time in the temple. At that time, I had been knocked unconscious for close to five (5) minutes. “Coincidentally” the CCTV footage I had been given by the […] prosecutor involved with the case had no time stamps as well as the handcuff to the temple punch was cropped out of the video. Imagine that I am seen being struck in the head over 20+ times and I am still conscious but the shot that KO's me is not available for the camera to pick up hmm […]

[para 11] The Public Body argues:

The video at issue shows how the interior space is configured in a day room [holding cell] (where the Applicant was placed after he was handled by the Correctional Peace officers) in a specific correctional center, in this case, CRC. If disclosed, the video would reveal the camera angles, potential blind spots, security mechanisms, tactical procedures used to respond to a specific type of event and the facility layout. Disclosure of the video could reveal the Centre’s security strategies and tactics including strategies and tactics displayed in this video. This would pose a security risk to staff, inmates and visitors. Disclosure would facilitate the escape by inmates, increase the risk of unauthorized contraband and increase the amount of violent altercations within CRC.

[para 12] The Public Body also states:

The Public Body submits that releasing the video footage allows for the possibility that the CCTV video or the security information (such as blind spots, security mechanisms and security procedures) could be passed along to other individuals who are currently in custody or may in the future be in custody at the Calgary Remand Centre. The possibility of the CCTV being shared or distributed, including the sharing and distribution of the security information contained within the

> CCTV, either directly to other individuals or by social media, raises a serious security concern for the Calgary Remand Centre.

[para 13] The Public Body argues that disclosure of the video at issue could enable individuals to identify blind spots in its camera system, the layout of the Calgary Remand Centre, as well as the techniques, tactics, and procedures employed by correctional peace officers. It reasons that the disclosure of such information could then be used to exploit vulnerabilities in the Calgary Remand Centre's security systems, and to anticipate what correctional pe+ace officers are likely to do in order to counter it. This could pose risks to staff, inmates, and visitors, and potentially enable inmates to escape. In addition, the Public Body reasons that knowledge of the camera blind spots could enable the exchange of contraband or increase the number of violent altercations at the Calgary Remand Centre.

[para 14] As it was unclear to me from the Public Body's evidence and submissions how the harms it projects would be likely to result from the disclosure of the video, I wrote to it *in camera* to obtain further evidence and explanation. In particular, I asked it questions as to whether other cameras were operating, even though any footage from such cameras had not been included in the video the Public Body created. I also asked it whether the cameras had been moved and asked it for current footage from the cameras that could be compared with the footage in the video. I also asked for a new copy of the video, as the copy I had been provided was missing content. The Public Body complied and provided a second copy of the video that included an additional segment, as well as photographs and stills to enable me to understand where the blind spots to which it refers in its submissions are located.

[para 15] To fall within the terms of the provisions the Public Body has applied, it must be established that disclosure of the video could reasonably be expected to facilitate the escape from custody of an individual who is being lawfully detained, facilitate the commission of an unlawful act or hamper the control of crime, harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

[para 16] I turn first to the question of whether disclosure of the video would reasonably be expected to facilitate the escape from custody of an individual who is being lawfully detained within the terms of section 20(1)(j).

Could disclosure of the video be reasonably expected to facilitate the escape from custody of an individual who is being lawfully detained?

[para 17] In Order F2022-46, the adjudicator determined that disclosure of information regarding security and security procedures will not meet the terms of section 20 if it lacks sufficient detail and is known to the public. She said:

> For the most part, I accept the Public Body's argument that the information in the records at issue has not been made public and/or is not routinely disclosed. The exception is the photos of prison weapons. It is not clear that the photos were taken at a correctional facility run by the Public Body;

at least one of those photos was copied from (or posted to) the internet. It seems possible that the other photos are also from an internet search. In any event, nothing in the photos reveals any sort of weaponry that cannot be readily located via an internet search. Further, the photos are of crude weapons made from everyday materials (for example, a sharpened stick or beverage container). I do not accept that a photo of a sharp object can be characterized as revealing "technical information relating to weapons or potential weapons" simply for the reason that the sharp object could be used as a weapon. Regarding the application of section 20(1)(k) to these pages, I assume the Public Body means to argue that an inmate could use the photos as a guide to create weapons. Some of the images are also difficult to decipher, such that it is not possible to determine how the implements were created. In my view, none of the photos shows anything that is not otherwise available to the public such that disclosing the photos could reasonably be expected to facilitate a crime. Given the ease with which such pictures of prison weapons can be located online, I do not accept that disclosing these photos could facilitate the commission of an unlawful act or hamper the control of crime. I make the same finding regarding the description of how prison weapons have been made in the past on page 127, as it is also general rather than specific, and also common knowledge.

In the Orders discussed above, section 20(1) (or equivalent sections in other jurisdictions) was found to apply where disclosure would reveal vulnerabilities in techniques, strategies and procedures used by law enforcement. The respective adjudicators accepted that disclosure of such information could permit countermeasures to be taken, that would undermine the efficacy of such techniques etc.

In Ontario Order PO-2332, the adjudicator noted that while some of the security measures discussed in the records were common sense, a knowledgeable person could identify absences of certain measures, or other deficiencies. In that case, the records at issue consisted of a security audit of a maximum security centre. It is reasonable to assume that a security audit would contain a detailed and comprehensive account of the centre's security arrangements.

The Public Body similarly states that the records reveal detailed information, such as information about protocol, surveillance tools and other technology.

However, in my view, much of the information in the records is not sufficiently detailed to meet the necessary standard; in other words, in many cases, the likelihood of one of the outcomes in section 20(1) cited by the Public Body resulting from disclosure is not considerably above a mere possibility.

[para 18] The Public Body argues:

The video at issue shows how the interior space is configured in a day room (where the Applicant was placed after he was handled by the Correctional Peace officers) in a specific correctional center, in this case, CRC. If disclosed, the video would reveal the camera angles, potential blind spots, security mechanisms, tactical procedures used to respond to a specific type of event and the facility layout. Disclosure of the video could reveal the Centre's security strategies and tactics including strategies and tactics displayed in this video. This would pose a security risk to staff, inmates and visitors. Disclosure would facilitate the escape by inmates, increase the risk of unauthorized contraband and increase the amount of violent altercations within CRC.

[…]

The Public Body determined that subsection 20(1)(j) applied to the record in question. The protected information displays the layout of the unit and hallways within the CRC. Locking mechanisms and staffing are displayed.

[para 19] I am unable to find that the video reveals sufficient information about the layout of the Calgary Remand Centre to be able to exploit a vulnerability in its security. The video is of some hallways in the Calgary Remand Centre and a holding cell. It is unclear from the video how these hallways relate to other areas of the Calgary Remand Centre or even to each other. Moreover, it is unknown, based on the evidence before me, whether there is a means of egress in the vicinity of the filmed area that would enable anyone to escape or help someone else to do so.

[para 20] The Public Body is concerned that disclosure of the video will reveal physical security mechanisms such as the way doors are opened and locked. The Public Body is also concerned that the video will reveal sensitive information about the layout of the Calgary Remand Centre. The video does not appear to provide detail regarding the locking mechanisms. If the Public Body is concerned that the locking mechanisms would in fact be identifiable to an expert, and that an image of doors could enable someone to exploit its systems in some way, it has made no submissions addressing this question. If, in fact, the video reveals an exploitable feature in its door opening mechanisms, the Public Body has not provided any evidence to explain how they could be exploited or how doing so could facilitate an escape. As well, as will be discussed in greater detail below, it has also not explained why it could not sever any such information from the video and provide the remainder to the Applicant.

[para 21] The evidence before me does not support finding that disclosure of the configuration of the room in which the Applicant was placed at the conclusion of the video -- the "day room" or "holding cell" --, would, in anyway, facilitate the escape of someone from the Calgary Remand Centre. It is unclear on the evidence before me what vulnerabilities the room configuration would reveal or why the Public Body believes that knowledge of any such vulnerabilities could then be employed to facilitate an escape.

[para 22] I do not mean to suggest that information about the layout or configuration of the Calgary Remand Centre could never be subject to section 20 – only that the Public Body has not demonstrated that any information derived from the video about its doors or locking systems or the configuration of rooms, could be exploited such that the harm contemplated by section 20(1)(j) could reasonably be anticipated to result.

Could disclosure of the video reasonably be expected to facilitate the commission of an unlawful act or hamper the control of crime?

[para 23] Cited above, the Public Body takes the position that disclosing the video will enable members of the public and inmates to identify camera blind spots. It reasons that inmates may exploit these blind spots which would "increase the risk of unauthorized contraband and increase the amount of violent altercations within CRC."

[para 24] In response to my request, the Public Body recorded still "1(b)" from the same camera that recorded the footage contained in the 2015 video. It also created still "1(a)", an image from the video, for comparison purposes. It asserts that the camera has

not been moved. It argues that the disclosure of the video would reveal a blind spot on the right hand side and at the bottom of the frame.

[para 25] From my review of the evidence the Public Body provided, I find that the camera angles in the footage from 2015 and the camera still from the same surveillance camera in 2023 are markedly different. This is illustrated by stills "1(a)" and "1(b)", which the Public Body submitted *in camera*. Still "1(a)" is taken from the 2015 video at issue.

[para 26] In comparing the two stills, I note that more ceiling is visible in the top of the frame of the 2015 video than is visible in 2023. Less floor is visible in the bottom of the frame of the 2015 video than is visible in 2023. A wall beside a counter is less visible on the right side of the frame in the 2015 video than it is in the 2023 still. The still taken in 2023 reveals more of the right side of the hallway than does the video at issue.

[para 27] I have not been provided the dimensions of the hallway that is the subject of the stills, but a conservative estimate would be that the still from the video of 2015 and the video itself, are missing at least twenty square feet of floor area visible in the 2023 still.

[para 28] A simple explanation for the differences in angles would be that the camera has been adjusted downward so that it now covers less ceiling area and more floor area than it did when the video was created in 2015. Moving the camera in this way would also affect the right and left margins. In saying this, I do not mean that the Public Body should not have adjusted the camera. The camera now covers more floor area than is viewable in the video, and the blind spot reduced, so that the camera can better serve its purpose. In other words, deficiencies in the original camera placement have been corrected. I note the differences between the video of 2015 and the still of 2023 because the Public Body denies moving the camera and makes submissions regarding the video at issue, as if it reflects the angles captured by the camera in its current position. This approach undermines the effectiveness of the Public Body's arguments in relation to the evidence, given the noticeable difference in camera angle in 2015 and 2023.

[para 29] In any event, the Public Body's primary concern is that disclosure of the video would reveal camera blind spots. It is concerned that these blind spots could then be exploited resulting in the harms contemplated by section 20(1)(k).

[para 30] Clearly, there are limits to what video cameras can capture. It is not clear to me that the video itself reveals blind spots. One would need to know that area not shown in a video was also not viewable by other means, to be identifiable as a blind spot in a security system.

[para 31] I note, too, that the CCTV cameras are not the only means by which inmates are observed in the areas shown in the video. The area has interior windows and glass doors through which inmates may be directly observed by guards and other staff members. While the Public Body argues that there is a small area not observed by CCTV

cameras, it is unclear from its evidence to what extent disclosure of the video would enable an individual to identify a blind spot. Even beyond the fact that the video at issue does not accurately represent the camera's current perspective, a person familiar with the Calgary Remand Centre could only conclude from the video that areas outside the frame are not covered by the camera that took the footage. Someone unfamiliar with the security systems in place in the Calgary Remand Centre would be unable to determine the areas not covered by a CCTV camera, as they are not visible. Identifying a blind spot in a security system requires more information about the system than can be provided by one video.

[para 32] I believe that the Public Body is concerned that if the video were released, inmates familiar with the area in which the surveillance camera that took the footage is located, could review the video to learn the area not covered by the cameras and then use that area to transact criminal business or commit violent acts without being detected.

[para 33] I am unable to accept this argument. The cameras (including the camera that recorded the first 7 ½ minutes of footage) covering the hallway in question are prominent. The area not captured by the cameras would be clear to anyone observing how they are placed, in the absence of the video. Moreover, even to someone who reviewed the video and also knew how the cameras were positioned in the hallway, it would be unknown what other security measures, including other cameras and correctional officers, the Public Body has in place to discourage criminal activity in the area covered by the camera. What would be known to such a person are all the glass security doors and windows with direct lines of sight to the area not covered by the surveillance cameras in the hallway. As a result, it is unlikely that the area not covered by the cameras would, in fact, be a desirable place to commit acts of violence or other crimes, or that such actions would not be detected immediately if someone tried to commit them in the camera blind spot.

[para 34] In *British Columbia Order F08-13*, an applicant requested her personal information from footage taken from a surveillance camera in a correctional facility. The Public Body in that case applied section 15(1) of British Columbia's *Freedom of Information and Protection of Privacy Act*, which is similar to Alberta's s. 20(1). In that case, the Public Body argued that the video revealed the presence of blind spots and that knowing the location of blind spots would result in attempts "to exploit these areas to ingest drugs, or harm themselves or others". The Adjudicator rejected this argument, stating:

> I agree with the public body that, at least in the circumstances of this case where there is evidence that the applicant intends to widely disseminate the information, it is appropriate to consider disclosure to the applicant as amounting to disclosure to the world. I also agree with the public body that the video surveillance system and the security features of the jail are part of the class of objects contemplated by s. 15(1)(l)'s reference to "property or system".
>
> As noted above, it appears that DVRs #2 and #3 contain the information of interest to the applicant. Each of these DVRs is shot entirely within a cell. The only concern raised by the Deputy Warden specific to these DVRs is the fact that the DVRs reveal some information about

> the camera's limitations: first, what portion of the cell cannot be seen by the security camera; and second, that some of the images are of poor quality.
>
> I agree that disclosure of gaps in the coverage of a surveillance system might compromise the effectiveness of such a system in some circumstances. However, in DVRs #2 and #3, the cells are small and the blind spots appear to be very limited. In addition, the nature of the blind spot is such that it is likely obvious to anyone who can see the camera's position and angle. Nothing in the evidence suggests that the cameras are hidden or inaccessible. Indeed, the evidence of the Deputy Warden is that inmates often try to disable the cameras. This suggests that they are easily identified. In the case of DVRs #2 and #3 then, there is nothing of significance about the cameras' limitations which will be disclosed by the footage which would not already be apparent to anyone in a position to take advantage of the blind spot. There is no clear and direct connection between the disclosure of the information in question and the alleged harm.
>
> […]
>
> Because DVRs #2 and #3 are limited to the interiors of single cells, they are also unlikely to give rise to the concerns cited by the public body in its submissions on the mosaic effect. I note, as well, that Commissioner Loukidelis has stated that the cases where the mosaic effect applies will be the exception and not the norm. In cases where it has been applied, there has been clear and convincing evidence that the evidence could be linked, and was intended to be linked, with already available information. In this case, there is only speculation that the information in any of the DVRs may be linked with other unidentified information that may or may not exist. None of the parties set out how the information in DVRs #2 and #3 might be linked with other information to present a security risk.
>
> While the safety and security of staff and others in the VCJ are undoubtedly of great importance, the concerns raised in the submissions of the public body and of the VPD do not establish a clear connection between the release of DVRs #2 and #3 and any risk of harm. The concerns raised in this regard are, to say the least, generalized and speculative. While I accept that the safety of officers and individuals in custody may be compromised if limitations in a security system are well-known, I do not, for the reasons set out above, accept that releasing DVRs #2 and #3 will reveal any such limitations. In coming to this conclusion, I have kept in mind the concerns the public body raised with respect to the possibility that the tapes might be technically enhanced and might be viewed alongside other information, including other DVRs. Arguably, such concerns are too speculative to form part of the determination regarding s. 15(1). However, even taking them into account, I find that the public body has not discharged its burden under s. 15(1).
>
> The VPD made virtually no specific submissions on the application of s. 15(1) to the specific DVRs in question. Its affidavit evidence states that "any DVR evidence" should be withheld on the basis that it could expose limitations in the security system and compromise the ability of staff to monitor individuals in custody. Section 15(1) clearly contemplates a harms-based, rather than a class exception. The VPD put forward no evidence which was "detailed and convincing enough to establish specific circumstances for the contemplated harm to result from the disclosure of the information". There is no explanation of how the disclosure of the information in DVRs #2 and #3 could lead to any of the harmful consequences alluded to, such as enabling prisoners to commit criminal acts, or exploiting the restraint devices that are in place.

[para 35] The foregoing decision was upheld at the Supreme Court of British Columbia by Russell J. in *British Columbia (Public Safety and Solicitor General) v. Stelmack*, 2011 BCSC 1244 (CanLII). The Court found it reasonable for the Adjudicator to find that a linkage between disclosure of the DVRs and the projected harms had not been established. I agree with the reasoning of the Adjudicator in British Columbia Order F08-13.

[para 36] For the reasons above, I am unable to say that disclosure of the video would be likely to result in acts of violence of the selling of contraband or drugs in the area not covered by the video.

Would disclosure of the video be reasonably expected to result in harm to the security of any property or system, including a building, a vehicle, a computer system or a communications system?

[para 37] The camera placement at the Calgary Remand Centre is a deliberate design choice and reflects decisions to have surveillance cameras capture particular areas, but not others, such as the area directly below a surveillance camera. It does not follow from the fact that certain areas are not caught by surveillance cameras that there is a vulnerability in the security of the Calgary Remand Centre or that these areas are not subject to other means of surveillance. Even if the camera blind spot were the result of design error, the Public Body could remedy the error by adding a camera to cover the area, if doing so reflects its security needs, or adjust the cameras to minimize the blind spot, as it appears to have done.

[para 38] In Order F2020-22, the Adjudicator determined that disclosure of landline numbers would not be likely to harm the security of the Calgary Police Service's telephone systems, even if individuals were to make harassing phone calls to these numbers. She said:

> Section 20(1)(m) applies where disclosure of information could reasonably be expected to harm the *security of a system or property*. The Public Body has not explained how receiving harassing phone calls from the Applicant or any other individual could *harm the security* of its phone systems. The Public Body has not mentioned the security of its phone systems, or how disclosing the contact information could reasonably be expected to harm the security of that system. As stated by the Supreme Court of Canada (cited above), there must be a reasonable expectation of probable harm, and the evidence must be 'well beyond or considerably above' a mere possibility.

[para 39] I agree with the Adjudicator in Order F2020-22 that section 20(1)(m) is concerned with the disclosure of information that could be reasonably expected to harm the security of property or the functioning of a *system*. Disclosing the video, even to someone with knowledge of the placement of the two cameras in the hallway, would not necessarily enable that person to harm or undermine the security of the Public Body's systems of surveillance or its systems of supervising inmates. If disclosure could reasonably be expected to have this result, the Public Body has not explained how it could.

[para 40] With regard to the video footage beginning 7:31 to the end of the video, I am unable to identify any blind spots that could be used in the manner contemplated by the Public Body in its submissions.

[para 41] I find that the disclosure of the video at issue alone could not reasonably be expected to reveal security vulnerabilities at the Calgary Remand Centre or enable anyone to compromise the effectiveness of the Public Body's systems within the terms of section 20(1)(m).

Security Procedures and Control Techniques

[para 42] The Public Body argues that security procedures and strategies would be revealed by disclosure of the video, which would potentially enable inmates to counter them, reducing their effectiveness. I agree that if this is so, section 20(1)(m) would be engaged.

[para 43] The Public Body argues that the video reveals how many guards responded to the incident, which would enable members of the public, or inmates, to learn how many guards are likely to respond to an incident. The video does not show how many guards could potentially have responded, or indicate how many guards are likely to respond to a given incident. The video only shows what was visible to the camera in a given space. For portions of the video, it is unknown how many corrections officers are present, from where they originated, or how they got there. I am unable to say that disclosure of the video would be likely to enable inmates to learn how guards will respond in any given incident.

[para 44] I asked the Public Body *in camera* to provide an explanation as to how the video reveals information regarding its control techniques. The Public Body indicated that Correctional Security Guards are trained in a finite number of control techniques and that it does not make the techniques it employs public. The Public Body argues that if members of the public learned about its control techniques by watching the video, they could train to counter them, rendering the techniques less effective. I infer from its previous arguments that the Public Body is not so much concerned that the public in general will learn its techniques and attempt to counter them, but that inmates of the Calgary Remand Centre will attempt to do so.

[para 45] The Public Body described one instance in the video that it considered to reveal a specialized control technique employed on the Applicant. It did not provide the time in which this technique occurs in the video. While I accept the opinion of the Public Body that there is an example of such a technique in the video, I am uncertain as to the extent that the technique is revealed, given the vagueness of the Public Body's submissions. I am also uncertain that disclosure could reasonably be expected to result in the harms to the Public Body's systems that the Public Body contemplates. To result in the harms the Public Body contemplates, the control technique could be countered by inmates or prospective inmates by gaining knowledge of the technique from the video, and this ability to counter the technique could then undermine the Public Body's control systems.

[para 46] As discussed in *Ontario (Community Safety and Correctional Services), supra*, a public body has the burden of proving that the harm it projects is reasonably probable.

[para 47] The Public Body also argues that after the takedown occurs, some of the footage reveals what it considers to have been a corrections officer's objective in order to take control of the Applicant. It argues that members of the public, after viewing this portion of the video could train to counter the officer's purpose. As the Public Body does not indicate that this portion of the video reveals a technique in which officers are trained, I am unable to say that the Public Body's control techniques would become known to the public if this portion of the video were viewed or that members of the public would have sufficient information from the video to train to counter the purpose the Public Body attributes to the officer.

[para 48] The Public Body did not answer my questions as to why it believes the control techniques and strategies it employs are unknown. It also did not explain how it ensures that its techniques and strategies are unknown, particularly when it may employ them in view of inmates.

[para 49] It is unclear to me, based on the evidence, that a member of the public or inmates would be able to identify the technique to which the Public Body refers as such, unless the member of the public also had the Public Body's submissions for the inquiry or already had training in self-defense or a similar discipline. Even if it were discernable, it is not reasonable to expect that the footage is sufficiently instructive such that members of the public or inmates would be likely to study it for the purposes of learning how to counteract the technique, or further, that if someone were to do this, they would be able to determine how to counteract the technique. It is also unknown, based on the evidence, that inmates would have the resources to train to counteract the technique. It is unclear that simply identifying the technique in the video could enable anyone to counter it successfully. The Public Body has not explained how the technique could be countered or indicated whether the technique could be countered easily. It seems possible that the Public Body trains officers in the technique because it is effective and not easily countered.

[para 50] Assuming that members of the public or inmates could identify the technique identified by the Public Body and then train to counter it, I am unable to say that this alone would undermine all the Public Body's control techniques. The Public Body's *in camera* submissions refer only to the harm that would result from *all* its control techniques being disclosed; they do not address the harm that could result from disclosure of only the technique it asserts is present in the video. The Public Body did not explain how disclosure of one control technique could reasonably be expected in a harm contemplated by section 20(1)(m). While I would agree with the Public Body that section 20(1)(m) could potentially apply if information about all, or a significant portion, of its control systems and techniques were revealed to the public, I am unable to say, based on the evidence, or the Public Body's arguments, that disclosure of the one technique identified by the Public Body would have the same effect. Rather, it appears likely that

the Public Body would simply use its other strategies and employ officers as necessary to control the situation should its use of the particular technique in a particular instance be countered. I am unable to say that disclosure of the technique in the video would make public all the Public Body's control systems, or render any of them, including the technique it states was used in the video, less effective.

[para 51] For the foregoing reasons, I find that it has not been established that section 20(1)(m) applies to the content of the video.

Severing

[para 52] In Review Report 21-04, the Information and Privacy Commissioner of Nova Scotia made the following comment with regard to a decision to withhold an entire video rather than to sever information thought to be subject to exceptions and to provide the remainder of the video to an applicant:

> Just as a paper record requires a line-by-line analysis, a video record requires a frame-by-frame analysis. To suggest that it is unreasonable to sever a video file is not adequate. Video surveillance is not new technology. It is reasonable to expect a public body collecting personal information in the form of a video record would also have a process by which to sever that record to ensure it can comply with the access to information legislation.

[para 53] I agree with the foregoing discussion. Section 6(1) of the FOIP Act states, in part:

> *6(1) An applicant has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.*
>
> *(2) The right of access to a record does not extend to information excepted from disclosure under Division 2 of this Part, but if that information can reasonably be severed from a record, an applicant has a right of access to the remainder of the record.*
>
> *[…]*

[para 54] The Public Body could have edited the video to obscure things such as the extent of blind spots, or the locking mechanisms of doors, as well as the technique it says was attempted to control the Applicant. It could then, in accordance with section 6(2), have provided the remainder of the video to the Applicant in response to his access request in a timely way.

[para 55] As I have found that sections 20(1)(j), (k), and (m) have not been shown to apply, I will not direct the Public Body to sever information from the video, but to provide it in its entirety. I make this point so that the Public Body considers severing information from video under section 6(2) when it receives similar access requests in the future so that an applicant may receive the information not subject to an exception to disclosure.

[para 56] To conclude, I find that the Public Body has not established that section 20(1)(j), (k), or (m) applies. I will direct it to give the Applicant access to the video in its entirety.

III. ORDER

[para 57] I make this order under section 72 of the Act.

[para 58] I order the Public Body to give the Applicant access to the video at issue in its entirety.

[para 59] I further order the Public Body to inform me within fifty days of receiving this order that it has complied with it.

Teresa Cunningham
Adjudicator