Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

ORDER MO-4033

Appeal MA19-00326

Chatham-Kent Police Services Board

March 29, 2021

Summary: In this order, the adjudicator finds that a request for access to a list of Chatham- Kent Police Services Board employee email addresses is not frivolous or vexatious under section 4(1)(b) of the *Municipal Freedom of Information and Protection of Privacy Act*. The adjudicator also finds that the information is not exempt under the law enforcement exemptions in sections 8(1)(a) (law enforcement matter), 8(1)(e) (endanger life or safety), 8(1)(i) (security), 8(1)(l) (facilitate escape from custody) or the exemption in section 13 (danger to safety or health). The adjudicator orders the police to disclose the record.

Orders and Investigation Reports Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, as amended, sections 4(1)(b), 8(1)(a), 8(1)(e), 8(1)(i), 8(1)(l) and 13; sections 5.1(a) and 5.1(b) of Regulation 823.

Cases Considered: Orders M-850 and MO-1168-I.

OVERVIEW:

[1] This appeal addresses whether the appellant's request for access to a list of email addresses of police employees is frivolous or vexatious, and whether the requested information is exempt under the discretionary exemptions in section 8 (law enforcement) or 13 (danger to safety or health) of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA or the Act*).

[2] Specifically, the appellant made a request under the *Act* for access to the email addresses of all employees of the Chatham-Kent Police Services Board (the police).

[3] The police conducted a search and located a responsive record. The police issued a decision denying access to the record on the basis of the discretionary law enforcement exemptions at sections 8(1)(a) (law enforcement matter), 8(1)(e) (endanger life or safety), 8(1)(i) (security), 8(1)(j) (facilitate escape from custody) and (8)(1)(l) (facilitate commission of an unlawful act), and the discretionary exemption at section 13 (danger to safety or health). The police also claimed that the information was exempt under section 11(d) (economic or other interests), but later withdrew this claim. Finally, the police also denied access because they claim that the request is frivolous or vexatious.

[4] The appellant appealed the police's decision to this office. A mediator was appointed to explore the possibility of resolution. During mediation, the police confirmed the grounds for their decision to deny access: the police say that the request is frivolous or vexatious within the meaning of section 4(1)(b) of the *Act*. In the alternative, the police rely on the discretionary exemptions at sections 8(1)(a), (e), (i) and (l), and section 13 to deny access. The police no longer rely on the exemption in section 8(1)(j), so that this exemption is removed as an issue in dispute.

[5] A mediated resolution of the appeal was not possible because the police maintained that the request is frivolous or vexatious as contemplated by section 4(1)(b) of the *Act* and section 5.1 of Regulation 823. The appeal was transferred to the adjudication stage of the appeal process, where an adjudicator began a written inquiry by seeking representations from the police on the issues and questions set out in a Notice of Inquiry. No representations from the appellant were sought. The appeal was then transferred to me to conclude the inquiry.

[6] In this order, I find that the police have not established that the appellant's access request is frivolous or vexatious under section 4(1)(b) of the *Act*. I further find that the information at issue is not exempt under the exemptions in sections 8(1) or 13 and order it to be disclosed to the appellant.

RECORDS:

[7] The record is a list of police employees' email usernames. The information at issue consists of the username portions of the email addresses that appear before the police's email domain name.

ISSUES:

A. Is the request for access frivolous or vexatious within the meaning of section 4(1)(b)?

B. Do the discretionary law enforcement exemptions at sections 8(1)(a), (e), (i) and/or (l) apply to the information at issue?

C. Does the discretionary exemption for threat to safety or health at section 13 apply to the information at issue?

DISCUSSION:

Issue A: Is the request for access frivolous or vexatious within the meaning of section 4(1)(b)?

[8] Section 4(1)(b) of the *Act* gives institutions a summary mechanism to deal with frivolous or vexatious requests. It states, in part, that:

> Every person has a right of access to a record or a part of a record in the custody or control of an institution unless,
>
> > the head is of the opinion on reasonable grounds that the request for access is frivolous or vexatious.

[9] This discretionary power in section 4(1)(b) can have serious implications for a requester's ability to obtain information under the *Act* and should not be exercised lightly.[1] On appeal to the IPC, the burden of proof is on the institution to provide sufficient support for the decision to declare the request frivolous or vexatious.[2]

[10] Section 5.1 of Regulation 823 under *MFIPPA* elaborates on the meaning of the terms "frivolous" and "vexatious:

> A head of an institution that receives a request for access to a record or personal information shall conclude that the request is frivolous or vexatious if,
>
> > (a) the head is of the opinion on reasonable grounds that the request is part of a pattern of conduct that amounts to an abuse of the right of access or would interfere with the operations of the institution; or
> >
> > (b) the head is of the opinion on reasonable grounds that the request is made in bad faith or for a purpose other than to obtain access.

[11] The police take the position that the appellant's request is frivolous or vexatious based on all of the grounds set out in section 5.1 of Regulation 823.

[12] For the reasons that follow, I reject the police's position.

Pattern of conduct that amounts to an abuse of the right of access or would interfere with the operations of the institution – Section 5.1(a)

[13] To establish the requirements of section 5(1)(a) of Regulation 823, a finding of a pattern of conduct on the part of the requester is required before proceeding to a

---

[1] Order M-850.

[2] Order M-850.

determination of whether the pattern of conduct either amounts to an abuse of the right of access, or would interfere with the police's operations.[3]

[14] Previous IPC orders have explored the meaning of the phrase "pattern of conduct." In determining whether a request forms part of a pattern of conduct that amounts to an abuse of the right of access, institutions may consider a number of factors, including the cumulative effect of the number, nature, scope, purpose, and timing of the requests.[4]

[15] To determine whether the appellant's request forms part of a pattern of conduct that would interfere with the police's operations, the police must establish that responding to the request would obstruct or hinder the range or effectiveness of the police's activities.[5] Interference is a relative concept, and must be judged on the basis of the circumstances of a particular institution. For example, a small municipality may face interference with its operations from a more limited pattern of conduct than a large provincial government ministry would, and the evidentiary onus on the institution would vary accordingly.[6]

Police's representations

[16] The police submit that the appellant has a history of frequent and abusive communications which are part of a pattern of conduct that shows an "abuse of other means of communication." The police submit that the appellant "constantly sends numerous E-mails, phone messages, letters and faxes to police regarding the same type of complaint." They say that they have received more than 200 communications from the appellant, and that the appellant's "barrage" of communications began after an arrest in 2018. As an example, the police say that in one month in 2019, the appellant sent 27 letters addressed to every supervisor of rank that contained "the exact same content." The police say that the appellant's written correspondence and phone calls are belligerent, accusatory, harassing, vulgar and laced with profanity. They say that most of the appellant's requests are outside the scope of what the police investigate, because they are either complaints or demands that matters be re-investigated. When dissatisfied with their response or actions, the police say that the appellant's communications increase.

[17] The police submit that the appellant is well aware of the different ways to contact them, and that he does not need additional means to do so. They argue that providing the appellant with access to the emails of all employees will serve to increase the amount of his emails, enable him to harass more staff who have no involvement with the appellant or his dealings with the police, and will allow the appellant to take advantage of contacting any employee at will.

---

[3] Order PO-4046.

[4] Orders M-618, M-850 and MO-1782.

[5] Order M-850.

[6] Order M-850.

[18] In addition to contacting the police directly, the police submit that the appellant also sends multiple communications and emails to other municipal offices. They say that those communications are then turned over to the police for their review and threat assessment. The police also submit that the appellant has already been declared a vexatious litigant by a court. The police argue that dealing with the sheer amount of the appellant's communications in the 18 months since they began, "continually and severely interfere[s] with" their daily operations and easily cost the equivalent of an officer's annual salary. If the record is disclosed, the police say the appellant's abusive conduct will continue.

[19] With respect to access requests in particular, however, the police submit that the appellant has made two prior requests for access to information under *MFIPPA* since 2014. Neither were considered to be frivolous or vexatious.

Analysis and findings

[20] Based on the evidence before me, I am not satisfied that the police have established, on reasonable grounds, that a pattern of conduct as contemplated by section 5.1(a) of Regulation 823 exists with respect to the appellant's request for access to the information at issue.

[21] Previous IPC orders have explored the meaning of the phrase "pattern of conduct." In Order M-850, for example, former Assistant Commissioner Tom Mitchinson wrote that:

> [I]n my view, a "pattern of conduct" requires recurring incidents of related or similar requests on the part of the requester (or with which the requester is connected in some material way). *(Emphasis added)*

[22] In addition to a high volume of communications they receive from the appellant (unrelated to requests for access to information under the *Act*), the police argue that "All requests from the Appellant are similar" in their content and insofar as they call for action like the arrest of lawyers, judges, justices of the peace, victims and other civilians. As for the timing of the request, the police say it relates to his 2018 arrest, after which the appellant "has displayed a clear animus toward police."

[23] I am mindful that the police's overriding concern is that disclosure of the record would make them, and specifically additional civilians and officers who have no dealings with the appellant, vulnerable to communication from, and therefore what the police say is harassment by, the appellant. However, the police's argument that the request is part of a pattern of abusive communications and therefore amounts to an abuse of the right of access or interferes with their operations, rests on the appellant's communications relating to matters outside of the access regime that is governed by *MFIPPA*. And while I acknowledge the police's concern that access under *MFIPPA* may result in an increase of other communications that the police consider problematic, that is not the test to establish a pattern of conduct for the purposes of section 4(1)(b) of the *Act*.

[24] Section 4(1)(b) speaks directly to the potentially frivolous or vexatious nature of requests for access to information under *MFIPPA*, and not about a requester's other communications with the institution. Regarding the appellant's requests for access – i.e.

requests that fall under the jurisdiction of *MFIPPA* – the police say that the appellant has only made two since 2014, neither of which were determined to be frivolous or vexatious.

[25] Order M-850 held that an unacceptable pattern of conduct includes "situations where a process is used more than once, for the purpose of revisiting an issue which has been previously addressed." While this may be the case with the appellant's communications that fall outside of the *Act* and by which the police feel harassed, this is not the case with the appellant's requests under *MFIPPA*, of which, as already noted, there have been two prior to the one that is before me in this appeal. The police give no evidence that the appellant has previously made a request under the *Act* for access to similar information or that the current request has been previously addressed in any other access request by the appellant under *MFIPPA*.

[26] Even if I were to find that the appellant's request is part of a pattern of conduct, the police have provided no evidence regarding any interference with their operations that would result from processing the request itself. Rather, the police's concern is that, once the request is processed and the information is disclosed, the appellant will engage in behaviour that will then interfere with the police's operations. I will discuss this further, below.

Bad faith or purpose other than to obtain access - Section 5.1(b)

[27] Section 5.1(b) of Regulation 823 sets out the second ground for establishing that a request is frivolous or vexatious. Under the "bad faith" portion of section 5.1(b), a request will qualify as frivolous or vexatious where the head of the institution is of the opinion, on reasonable grounds, that the request is made in bad faith. If bad faith is established, the police need not demonstrate a "pattern of conduct."[7]

[28] To qualify as a "purpose other than to obtain access," it must be established that the requester has an improper objective above and beyond a collateral intention to use the information in some legitimate manner.[8]

[29] The term "bad faith" has been defined in Order M-850 as:

> The opposite of "good faith", generally implying or involving actual or constructive fraud, or a design to mislead or deceive another, or a neglect or refusal to fulfil some duty or other contractual obligation, not prompted by an honest mistake as to one's rights, but by some interested or sinister motive. … "bad faith" is not simply bad judgment or negligence, but rather it implies the conscious doing of a wrong because of dishonest purpose or moral obliquity; it is different from the negative idea of negligence in that it

[7] Order M-850.

[8] Order MO-1924.

> contemplates a state of mind affirmatively operating with furtive design or ill will.[9]

[30] Previous orders have found that an intention by the requester to take issue with a decision by an institution, or to take action against an institution, is not sufficient to support a finding that the request is frivolous or vexatious on the basis of "bad faith."[10]

Representations

[31] The police argue that the appellant wishes to obtain all police employees' emails "other than in a professional capacity and…in bad faith." The police state that the "spamming and deluge of messages" are motivated by the appellant's dissatisfaction with the outcome of a number of his past negative contacts with the police and that his request has a purpose other than to obtain access.

[32] The police submit that the appellant's email history is abusive, irresponsible and unprofessional. The police submit that the appellant's emails violate their email and internet usage and IT policies. They say that the appellant has refused any direction from police regarding police procedures regarding the use of emails (and especially the filing of complaints). The police also submit that the appellant may have personal or health circumstances that may affect his communications,[11] but that when they give the appellant necessary contact information, he acts in bad faith by responding with the "incessant flurry" of emails.

[33] The police say that, while they share their email addresses with members of the public during investigations or while performing their job duties (in the case of civilian employees), police officers and staff do not randomly share emails with the public. They say that the appellant's misuse of the necessary contact information he receives as part of his dealings with police supports a finding that bad faith is behind his current request.

Analysis and findings

[34] Having reviewed the police's representations, I do not find sufficient basis to conclude that the appellant's request is made in bad faith or for a purpose other than to obtain access.

Bad faith

[35] Applying the definition of bad faith referred to above, I find that there is insufficient evidence before me to support a finding of bad faith on the part of the appellant in requesting access to the information at issue. As already noted, the IPC has interpreted "bad faith" as implying the "conscious doing of wrong because of dishonest purpose or

---

[9] Order M-850.

[10] Orders MO-1168-I and MO-2390.

[11] I have not summarized these as they are the appellant's personal information.

moral obliquity." Bad faith "contemplates a state of mind affirmatively operating with furtive design or ill will."[12]

[36] While I acknowledge the police's frustration with the appellant's high level of contact with their office, I have insufficient evidence to conclude that the appellant is motivated by some dishonest purpose. The police's reliance on the bad faith criterion appears tied to their belief that the appellant is sending communication (outside of the access regime provided for in *MFIPPA*) that is deliberately abusive. However, there is no evidence before me to demonstrate that the appellant is motivated by a dishonest purpose, or that his various emails and complaints to the police are deliberately malicious or fraudulent. Rather than having a dishonest purpose or being motivated by malice, the police's representations suggest that the appellant's request may be mitigated by personal or health struggles.

[37] I therefore find that the police have failed to establish that the appellant's request for access to the information in the record at issue was made in bad faith for the purposes of section 5.1(b) of Regulation 823.

Purpose other than to obtain access

[38] A request is made for a purpose other than to obtain access if the requester is motivated not by a desire to obtain access, but by some other objective. Where a request is made for a purpose other than to obtain access under section 5.1(b), it can be deemed to be frivolous or vexatious without the institution having to demonstrate a pattern of conduct.[13]

[39] Previous IPC orders have found that the fact that the request for access is motivated by an intention to take issue with a decision made by the institution or to take action against an institution is not sufficient to support a finding that the request is frivolous or vexatious.[14]

[40] I am mindful of the police's concerns that the appellant intends to use the information to intensify his communications with them and that granting access would give the appellant the means to contact a wider audience. The concern, however, that the appellant will use the information to contact the police (or, stated another way, contact *more* police and staff) is not an illegitimate exercise of the appellant's right of access to information. Once it is determined that a request is made for the purpose of obtaining access, this purpose is not contradicted by the possibility that the requester may also intend to use the information in a way that might have the result of antagonizing the police.

---

[12] Order M-850.

[13] Order M-850.

[14] Orders MO-1168-I and MO-2390.

[41] As stated by Adjudicator Laurel Cropley in Order MO-1168-I, there is nothing in the *Act* that delineates what a requester can and cannot do with information once access has been granted to it. The fact that the appellant may use the information in a manner that is disadvantageous to the police does not mean that his reasons for using the access scheme in the *Act* are not legitimate. There is no evidence before me that the appellant is acting with some dishonest or illegitimate purpose or goal, even if disclosure may result in more communications with the police.

Conclusion

[42] The tests under section 5.1 of Regulation 823 set a high threshold. I find that this threshold has not been met in the circumstances of this appeal and that the police have not established reasonable grounds for finding that the appellant's request for access is frivolous or vexatious within the meaning of section 4(1)(b) of the *Act*.

Issue B: Do the discretionary law enforcement exemptions at sections 8(1)(a), (e), (i) and/or (l) apply to the information at issue?

Preliminary issue

[43] As a preliminary issue, I have considered whether the information at issue is personal information as defined in section 2(1) of the *Act*.[15] This is because, once it has been determined that a record contains personal information, section 14(1) of the Act prohibits its disclosure unless one of the exceptions listed in section 14(1) applies. Section 2(1) defines "personal information" to mean recorded information about an identifiable individual that includes the individual's name "if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about" them.[16] Section 2(2.1) of the *Act*, however, states that personal information "does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.

[44] The police have not claimed that the information at issue is personal information and I find that it is not. As noted above, the record contains a list of the username portions of the email addresses of police employees. I have reviewed the record and am satisfied that it contains the names (in the form of an email username) of identifiable individuals in their business, professional or official capacity and that disclosure of this information would not reveal other personal information about them. Given my conclusion that this is not personal information under the *Act*, I will go on to consider whether the discretionary exemptions claimed by the police apply.

---

[15] The police were not asked to submit representations on the application of the definition of "personal information" in section 2(1) of the *Act*, nor have they claimed that it is.

[16] Section 2(1)(h).

The exemptions at sections 8(1)(a), (e), (i) and (l)

[45] In the alternative to their claim that the request is frivolous or vexatious under section 4(1)(b), the police rely on the law enforcement exemptions at sections 8(1)(a), (e), (i) and/or (l) to deny access to the information at issue.

[46] Sections 8(1)(a), (e), (i) and (l) state that:

> A head may refuse to disclose a record if the disclosure could reasonably be expected to,
>
> (a) interfere with a law enforcement matter;
>
> (e) endanger the life or physical safety of a law enforcement officer or any other person;
>
> (i) endanger the security of a building or the security of a vehicle carrying items, or of a system or procedure established for the protection of items, for which protection is reasonably required;
>
> (l) facilitate the commission of an unlawful act or hamper the control of crime.

[47] The term "law enforcement" is used in several parts of section 8 and is defined in section 2(1) as follows:

> "law enforcement" means,
>
> (a) policing,
>
> (b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
>
> (c) the conduct of proceedings referred to in clause (b).

[48] The term "law enforcement" has covered a variety of situations, including a municipality's investigation into a possible violation of a municipal by-law,[17] and a police investigation into a possible violation of the *Criminal Code*.[18] Generally, the law enforcement exemption must be approached in a sensitive manner, recognizing the difficulty of predicting future events in a law enforcement context.[19]

---

[17] Orders M-16 and MO-1245.

[18] Orders M-202 and PO-2085.

[19] *Ontario (Attorney General) v. Fineberg* (1994), 19 O.R. (3d) 197 (Div. Ct.).

[49] It is not enough, however, for an institution to take the position that the harms under section 8 are self-evident from the record or that the exemption applies simply because of the existence of a continuing law enforcement matter.[20] The institution must provide detailed evidence about the potential for harm. It must demonstrate a risk of harm that is well beyond the merely possible or speculative although it need not prove that disclosure will in fact result in such harm. How much and what kind of evidence is needed will depend on the type of issue and seriousness of the consequences.[21]

Representations

[50] As I have already noted, the police submit that, in the approximately 18 months following his arrest in 2018, the appellant made over 200 contacts with them by email, mail, fax or phone. In addition to direct correspondence, the police say that they also receive the appellant's communications from other municipal offices (to monitor for activities and possible threats). The police say that the appellant's various communications interfere with their operations as a law enforcement agency by presenting a significant drain on resources.

[51] The police also say that the appellant has created safety issues when he has attended their building, and that they have at times been called to assist when the appellant has attended other municipal buildings and antagonized staff. For example, the police submit that they have been called to assist at the local provincial court house when the appellant gave administrative staff "a hard time," and had to be supervised by police while he completed his matters before being escorted out.

[52] The police submit that, in addition to police officers, they employ civilian staff who, unlike more seasoned officers, might be more affected by the appellant's communications. The police submit that the appellant's emails violate their email and internet use and corporate IT policies and that, as an employer, the police must protect their staff from harassing conduct.[22]

[53] Finally, the police submit that, based on his past behaviour, there is no doubt that the appellant will continue his barrage of emails and that disclosure of the record will give the appellant another means of "bombarding" police personnel with harassing and spamming emails.

Analysis and findings

[54] As noted above, the police must provide detailed evidence about the potential for the harms specified in section 8(1)(a), (e), (i) and (l). Establishing the exemptions in section 8 of the *Act* requires that the expectation of one of the enumerated harms coming

---

[20] Order PO-2040 and *Ontario (Attorney General) v. Fineberg*, cited above.

[21] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner),* 2014 SCC 31 (CanLII) at paras. 52-4.

[22] I note that the policy excerpts provided with the police's representations apply to members of the police force, and not to the public.

to pass should a record be disclosed not be fanciful, imaginary or contrived, but based on reason.[23]

[55] Having this standard in mind, and based on my review of the record and the police's representations, I am not persuaded that the police have established that disclosing the record could reasonably be expected to result in any of the harms contemplated by the section 8(1)(a), (e), (i) or (l) exemptions.

Section 8(1)(a): law enforcement matter

[56] In order for the exemption in section 8(1)(a) to apply, the police must provide evidence of an ongoing or existing law enforcement matter.[24] This exemption does not apply where a matter is completed, or where the alleged interference is with "potential" law enforcement matters.[25]

[57] Although "matter" may extend beyond a specific investigation or proceeding,[26] the police have not provided evidence to establish the existence of any law enforcement matter. The police's representations focus on the potential increase in emails they expect from the appellant if he has access to more email addresses through disclosure in this appeal. They submit that, in one instance, the appellant singled out supervisors of rank and sent 27 copies of the same six page letter to each, requesting that the police either open investigations or bring charges against court or law enforcement officials. In other instances, the police say that the appellant sent various correspondence to the police asking that officers and other individuals be arrested, or making various complaints about the police. They say that dealing with the amount of the appellant's communication is costly and time consuming. However, I do not consider this to be evidence of an existing or ongoing law enforcement matter as that phrase has been interpreted under section 8(1)(a). As the police have not provided sufficient evidence to establish that disclosure could reasonably be expected to interfere with an ongoing or existing law enforcement matter, I find that section 8(1)(a) does not apply.

Section 8(1)(e): endanger life or safety

[58] In order for the exemption in section 8(1)(e) to apply, the police must provide evidence demonstrating that disclosure of the record could reasonably be expected to endanger the life or physical safety of a law enforcement officer or any other person. The term "person" is not limited to a particular identifiable individual, and may include the

---

[23] Orders PO-2099 and MO-2986.

[24] Order PO-2657.

[25] Orders PO-2085 and MO-1578.

[26] *Ontario (Ministry of Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner),* [2007] O.J. No. 4233 (Div. Ct.).

members of an identifiable group or organization.[27] While subjective fear is a potential consideration, it may not be enough to justify the exemption.[28]

[59] I find that the evidence before me falls short of demonstrating that disclosure of the record could reasonably be expected to endanger the life or safety of any individuals, whether police employees or otherwise. The police submit that the appellant has sent concerning emails that the police have had to review, and that he has created disturbances when attending at police or other offices. The police submit that disclosure of the record will enable the appellant to send more repetitive, unsolicited and inappropriate complaints. While seasoned officers can better handle the appellant's abuse, the police say that not all employees can, and that disclosure of the record will reduce their ability to protect staff from an onslaught of unsolicited communication. The police say that a senior professional standards officer currently vets the appellant's communications, which is already costly and time-consuming; they say that these costs will only increase once the appellant sends more emails. The police also submit that, on one occasion, the appellant placed his hand on an officer's arm while at the police station, although neither the officer nor police took any action, apart from escorting the appellant out.

[60] The police's representations do not describe a connection between the appellant sending emails (sent using disclosed email addresses) and his actions or conduct when attending a police station or other municipal office. In the circumstances, the police have not provided sufficient evidence on which I can conclude that the disclosure of the email addresses at issue could reasonably be expected to endanger the life or safety of any individual or organization under section 8(1)(e) of the *Act*.

Section 8(1)(i): endanger security of a building or vehicle

[61] To establish that section 8(1)(i) applies, the police must provide sufficient evidence for me to conclude that disclosure of the record could reasonably be expected to endanger the security of a building, vehicle, system or procedure established for the protection of items and, further, that such protection is reasonably required. In support of their position, the police point to the appellant's conduct when attending public buildings. As noted above, the police submit that they have been called to assist when the appellant has given court house staff "a hard time." The police also submit that the appellant has ignored their direction on the procedure for filing complaints, and that disclosing the record will increase the appellant's communication with them. However, this communication is limited to email communication in particular, and the police do not explain how disclosure of the record and access to email usernames are related to the appellant's behaviour at their or another building.

[62] I am not persuaded that the examples cited by the police support a finding that there is a reasonable expectation that disclosure of the record could reasonably be expected to endanger the security of a building, vehicles, systems or procedures established for the protection of items. I therefore find that section 8(1)(i) does not apply.

---

[27] Order PO-1817-R.

[28] Order PO-2003.

Section 8(1)(l): facilitate commission of an unlawful act

[63] For the exemption at section 8(1)(l) to apply, the police must provide evidence to demonstrate that the disclosure of the record could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of crime. The police speculate that giving the appellant access to more police contact information will result not only in a greater volume of communications from the appellant, but that those communications will have more recipients. As noted above, although the police say they share their email addresses with the public in the course of investigations (or, in the case of civilian employees, as part of their job-related duties), they submit that they do not disclose these emails randomly and that disclosing the record will simply give the appellant "another avenue of bombarding [them] with 'harassing' and spamming emails." It is clear that the police are aggravated and frustrated by the appellant's contacts. However, there is no suggestion by the police that the appellant's communications have risen to the level of being unlawful, nor is there any suggestion that access to the email addresses might change that quality of the appellant's contacts, as opposed to their quantity. Based on the evidence before me, I am not persuaded that disclosure the list of email addresses could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of crime, and I therefore find that exemption 8(1)(l) does not apply.

[64] I find that the harms identified by the police are insufficient to establish that the exemptions is section 8(1) apply to the record. Because speculation of possible harm is not sufficient to meet the requirements of the section 8 exemptions, I find that the record does not qualify for exemption under sections 8(1)(a), (e), (i) or (l).

Issue C: Does the discretionary exemption for threat to safety or health at section 13 apply to the information at issue?

[65] The police raised section 13 as a further alternative exemption claim to deny access to the requested information. This section states that:

> A head may refuse to disclose a record whose disclosure could reasonably be expected to seriously threaten the safety or health of an individual.

[66] For this exemption to apply, the police must provide detailed evidence about the potential for harm. They must demonstrate a risk of harm that is well beyond the merely possible or speculative, although they need not prove that disclosure will in fact result in such harm. How much and what kind of evidence is needed will depend on the type of issue and seriousness of the consequences.[29]

Representations

[67] In support of their reliance on the "danger to safety or health" exemption in section 13, the police have described some of their prior interactions with the appellant. Although I have reviewed the police's representations regarding those interactions, I have not

---

[29] *Ontario (Community Safety and Correctional Services v. Ontario (Information and Privacy Commissioner),* 2014 SCC 31 (CanLII) at paras. 52-4.

summarized them for the purposes of this order, because they contain personal information about the appellant.

[68] In summary, however, the police claim that the appellant's actions during some of his interactions with the police (including other police forces) pose threats to the safety and health of officers and civilians.

Analysis and findings

[69] The test under section 13 is similar to the test under section 8(1)(e). Given the similarity of the police's submissions on this issue with their submissions on the application of section 8, and for similar reasons, I find that section 13 does not apply.

[70] I find that the police have failed to prove that disclosure of staff email usernames could reasonably be expected to seriously threaten the safety or health of an individual, whether a police officer, the appellant or another civilian. The examples cited by the police describe discrete incidents alleging, for example, the appellant's failure to cooperate with the police.

[71] Apart from the anticipated increase in what the police say are already numerous communications from the appellant, the police have not demonstrated a risk of harm, or a harm that is well beyond the merely possible or speculative, as required for section 13 to apply.[30] The police have not demonstrated that these examples are connected to the appellant's communications, except to the extent that the appellant might have used some of those communications to complain about the police's actions. Further, I am unable to infer such a risk based on the contents of the record itself. I therefore find that the record does not qualify for exemption under section 13.

[72] Since I have found that the request is not frivolous or vexatious under section 4(1)(b) of the *Act*, with section 5.1 of Regulation 823 and that the exemptions in section 8 and 13 do not apply to the record, I order it disclosed to the appellant.

ORDER:

1. I order the police to disclose the record at issue to the appellant by **April 29, 2021**.
2. I reserve the right to require the police to provide me with a copy of the record disclosed to the appellant, in order to verify compliance with order provision 1.

Original Signed by: March 29, 2021

Jessica Kowalski
Adjudicator

[30] *Ontario (Community Safety and Correctional Services v. Ontario (Information and Privacy Commissioner),* 2014 SCC 31 (CanLII) at paras. 52-4.