ALBERTA
INFORMATION AND PRIVACY COMMISSIONER

REQUEST TO DISREGARD F2020-RTD-01

May 8, 2020

EDMONTON POLICE SERVICE

Case File Number 012484

[1] The Edmonton Police Service (EPS or the Public Body) requested authorization under section 55(1) of the *Freedom of Information and Protection of Privacy Act* (the FOIP Act) to disregard two access requests made by an individual (the Applicant).

[2] EPS also requested authorization to disregard future requests of a similar type and to have a "cooling off" period of two years in which it does not have to respond to any access requests from the Applicant.

[3] For the reasons outlined in this decision, I have decided to authorize EPS to disregard the Applicant's two access requests and to disregard future access requests of a similar type. However, at this time, I do not authorize EPS to disregard all access requests from the Applicant for the requested two year "cooling off" period.

Commissioner's authority

[4] Section 55(1) of the FOIP Act gives me the power to authorize a public body to disregard certain requests. Section 55(1) states:

> *55(1) If the head of a public body asks, the Commissioner may authorize the public body to disregard one or more requests under section 7(1) or 36(1) if*
> *(a) because of their repetitious or systematic nature, the requests would unreasonably interfere with the operations of the public body or amount to an abuse of the right to make those requests, or*
> *(b) one or more of the requests are frivolous or vexatious.*

[5] Under section 55 of the FOIP Act, the Public Body has the burden to establish that the conditions of either section 55(1)(a) or (b) have been met.

Background

[6] On June 3, 2019, EPS received two access requests under FOIP from the Applicant as follows:

2019-P-395

1) I would like to see any and all information, regardless of format, relating to my name and/or address where I am listed in an EPS file #, and I did not call EPS for service. This will also include Event Chronology. Time Period: April 1, 2019 to April 30, 2019

2) I would like to see any and all information, regardless of format, regarding communication of any sort, in relation to my name and/or address that was received by/distributed by the following:
   - [5 named EPS members]
   - Professional Standards Branch
   - Southeast Community Liaison Sgt for Sector 1
   - Southeast Community Liaison Constable for Sector 1
   - Organizational Security
   - Professional Standards Branch
   - Legal Services Branch

   Time Period: April 1, 2019 to April 30, 2019

2019-P-396

1) I would like to see any and all information, regardless of format, relating to my name and/or address where I am listed in an EPS file #, and I did not call EPS for service. This will also include Event Chronology. Time Period: May 1, 2019 to May 31, 2019

2) I would like to see any and all information, regardless of format, regarding communication of any sort, in relation to my name and/or address that was received by/distributed by the following:
   - [5 named EPS members]
   - Professional Standards Branch
   - Southeast Community Liaison Sgt for Sector 1
   - Southeast Community Liaison Constable for Sector 1
   - Organizational Security
   - Professional Standards Branch
   - Legal Services Branch

   Time Period: May 1, 2019 to May 31, 2019

[7] The two access requests are essentially identical, other than the months specified in the time period.

[8] On June 21, 2019, I received EPS' request under section 55(1) of the FOIP Act to disregard access requests 2019-P-395 and 396. The Applicant was copied on this request, other than certain portions which were redacted pursuant to sections 20(1)(a) and (f) of the FOIP Act. On July 31, 2019, I confirmed EPS' decision to redact those portions of its

submission and accepted them *in camera*. I received the Applicant's comments on August 30, 2019.

[9] This decision refers only to the portions of EPS' submission that were made available to the Applicant; however I have considered all of the information before me.

EPS' Submissions

[10] In its submission that was provided to the Applicant, EPS stated in part:

> This Applicant has created very contentious issues for the EPS. While we respect and validate all of our Applicant's [sic] rights to fair and transparent access to information, this Applicant has pushed us well past the point of reasonable use of EPS resources. We have determined that her FOIPP requests are a part of a process the Applicant uses to frivolously engage our employees to the point of harassment, keeping them from their legitimate police work.
>
> The Applicant is a heavy user of EPS services. I have attached a listing from the EPS records management system EPROS to demonstrate the number of recorded occurrences involving the Applicant (tab 2). This list does not include events that were concluded without case files.
>
> [Information redacted under sections 20(1)(a) and (f) of FOIPP]
>
> To summarize, […] the Applicant has created false 911 calls for service. She has created counterfeit identities and fake check-on-welfare calls or other calls to her neighborhood; she has created fake Facebook accounts and posted messages on the SE Division Facebook page; has subsequently sent emails through to EPS members, as herself and as these other identities; and then FOIPPed the results of these communications.
>
> The Applicant then submits (on a monthly basis) FOIPP requests for information about who has called in about her and what record, in any format, named members have created about her. In total, the Applicant has submitted 68 FOIPP requests over the past 10 years, 57 since 2016.
>
> The FOIPP requests themselves have become a part of this systemic abuse of EPS services. As there have been so many requests, I will follow one particular case occurrence [references and supporting documents redacted]:
>
> - The Applicant generates an unnecessary check on welfare care, and an EPS member is obligated to attend the Applicant's house to confirm her well-being
> - The Applicant continues to contact the member and the member's supervisor through emails following the attendance, threatening Professional Standards Branch (PSB) involvement unless they respond.
> - The Applicant FOIPPs all records relating to the occurrences.
> - The Applicant then frivolously contacts PSB and then FOIPPs the PSB file.

- The Applicant sends correction requests to members despite being advised of the EPS request-for-correction process, and then re-FOIPPs the case file.
- The Applicant continues to FOIPP on a monthly basis, the member's records.

These check on welfare and lawn sign complaint investigations are the definition of frivolous and vexatious. This, coupled with the time spent on searching for records created by these fictitious calls for service, have been the cause of much frustration among members dealing with her numerous files. Member's time should be spent on legitimate law enforcement activities, not searching for records that have, on several occasions, been found not to exist – also a section 55(1)(a) consideration.

Of perhaps greater concern is the malicious software the Applicant has been sending repeatedly to the EPS through her emails. This malware causes the recipient's computer system to crash when they attempt to print or forward her email. This has occurred when members have attempted to respond to her FOIPP requests. [examples redacted]

The Applicant's malware became such a distraction to EPS members that Legal Services Branch issued a directive to the Applicant to only communicate with the Service via writing or telephone.

A reasonable person should know that there is no sound basis for creating false calls, harassing members with numerous emails about those false calls, and then FOIPPing the resulting records, if any. A reasonable person would not repeatedly send malware to the police, which triggers when the member tries to respond to her FOIPP requests.

Based on the above, we request to disregard FOIPP Requests 2019-P-395 and 2019-P-396 and also any future requests that involve:

> "*…any and all information, regardless of format, relating to my name and/or address where I am listed in an EPS file #, and I <u>did not</u> call EPS for service"*
>
> *"…any and all information, regardless of format, regarding communications of any sort, in relation to my name and/or address that was received by/distributed by the following [named members]"*

We also request a cooling off period of two (2) years in which we do not respond to any FOIPP requests from the Applicant in order to discourage fictitious calls for service. The cooling off period would also serve to reduce her harassment of the members who attend her calls for service. This ability to disregard for a set time period is within the Commissioner's authority as per IPC file F3885.

I trust you will understand the gravity of this situation and the strain that this Applicant has placed and continues to place, on EPS resources.

[11] EPS provided numerous records supporting its submission, most of which were also provided to the Applicant and the remainder I accepted *in camera*.

The Applicant's submissions

[12] As noted above, portions of EPS' request were redacted under sections 20(1)(a) and (f) of the Act, and were not provided to the Applicant. I accepted these redacted portions *in camera.* In her response, the Applicant pointed out that she would be unable to respond to information that she was unable to read in EPS' submission.

[13] The Applicant stated, in part:

1) EPS has alleged that I designed malware and sent emails to them with this malware, designed to freeze their computer systems.

   This is in fact incorrect. EPS chose to believe that I did this.

   I have never designed any malware, nor have I ever knowingly used any malware.

   What EPS' IT branch could have done, is to have contacted me to figure out what the issue was. I did respond to EPS' [name redacted] (Legal Branch) in response to his letter in this regard (late 2018). I did inform him that I was certain it was not illegal to use "read receipt" notifications in emails.

   I also mentioned that I was the Executrix for a complex Estate and had used "read receipt" notifications in emails related to Estate matters for almost 8 years and never had anyone informed me that their computer system froze.

   The law firm that was dealing with the Estate matters also used "read receipt" notifications in their emails in some, if not all instances.

   I would suggest that EPS contact www.getnotify.com about their "read receipt" notification system. That is where the issue lies and not with the people who use that service.

   No one from the FOIP unit ever contacted me to inform that they had read an email and that it had frozen their system.

   I could find nothing in the FOIP Act of Alberta that would prohibit someone from submitting a FOIP request because they had used a "read receipt" notification.

   How does the fact that I used a service to get a 'read receipt' notification become a reason to deny FOIP requests?

2) Why did I include a number of names in the FOIP requests?
   I was informed by a FOIP Unit employee that they (EPS) have over 1,700 members so I would have to narrow my request. That is why I had to 'guesstimate' at times when listing members in a FOIP request. Esp. relating to PSB files from 2018 and 2019.

3) I will gladly communicate 'in camera' with OIPC in regards to the PSB files of 2018 and 2019 and the FOIP requests about those files.

> I will also gladly communicate 'in camera' with the OIPC about my reasons for further FOIP requests from August, 2018 into 2019.
>
> I have concerns about disclosing any more names of EPS employees in this regard (not the ones listed in the PSB complaints) to provide further clarification.
>
> Thank you for your consideration in this regard.

[14] The remainder of the Applicant's submission focuses on various 'Occurrences' listed at Tab 2 of EPS' submission, providing clarification and occasionally disputing the information.

Application of section 55(1) of the FOIP Act

[15] Generally, when a public body asks for authorization to disregard an access request, its submission must be shared with the applicant in its entirety. Exceptions can be made. Given the nature of the Public Body's evidence and submissions in this case, it chose to redact certain portions from the Applicant under section 20(1)(a) and (f) of the FOIP Act. I confirmed that decision and accepted those portions *in camera*. In my opinion, the *in camera* information provided by EPS does not add anything new to the submissions that were shared with the Applicant; rather, the *in camera* information substantiates and provides additional support to EPS' submissions that were provided to the Applicant.

[16] The rationale behind section 55 was explained by former Commissioner Work when he stated:

> The FOIP Act was intended to foster open and transparent government (Order 96-002 [pg. 16]). Section 2(a) and section 6(1) of the FOIP Act grants individuals a right of access to records in the custody or under the control of a public body. The ability to gain access to information can be a means of subjecting public bodies to public scrutiny.
>
> However, the right to access information is not absolute. The Legislature recognizes there will be circumstances where information may be legitimately withheld by public bodies and therefore incorporated specific exceptions to disclosure to the FOIP Act. Section 2(a) of the FOIP Act states the right of access is "*subject to limited and specific exceptions*" as set out in the FOIP Act. Section 6(2) of the FOIP Act states that the right of *access "does not extend to information excepted from disclosure*" under the FOIP Act.
>
> In my view, the Legislature also recognizes that there will be certain individuals who may use the access provisions of the FOIP Act in a way that is contrary to the principles and objects of the FOIP Act. In Order 110-1996, the British Columbia Information and Privacy Commissioner wrote:
>
> *"…The Act must not become a weapon for disgruntled individuals to use against a public body for reasons that have nothing to do with the Act…"*

> Section 55 of the FOIP Act provides public bodies with a recourse in these types of situations.[1]

[17] Although access to information rights are quasi-constitutional, they are not unlimited. No one has a right to make abusive access requests.

Section 55(1)(a) – Repetitious or systematic in nature

[18] A request is "repetitious" when it is made for the same records or information more than once. Although the Applicant uses similar language in her access requests, the evidence before me shows that they are for different time periods.

[19] Requests that are "systematic in nature" include a pattern of conduct that is regular or deliberate. In this case, EPS described the Applicant's pattern of conduct in its submission. It also provided further detail through an example of one particular occurrence starting from an initial unnecessary check on welfare call resulting in EPS attendance through to multiple access and correction requests. I am satisfied, based on EPS' evidence and submissions that this pattern of conduct is both regular and deliberate, and is therefore systematic in nature.

Section 55(1)(a) – Unreasonably interfere with the operations of the public body or amount to an abuse of the right to make those requests

[20] Under section 55(1)(a), the requests must also unreasonably interfere with the operations of the public body or amount to an abuse of the right to make those requests.

[21] Although EPS mentioned the amount of time it has spent responding to the Applicant's numerous FOIP requests over the past decade, there is insufficient evidence before me to find that responding to these requests would unreasonably interfere with its operations. However, EPS has provided sufficient evidence for me to determine whether the systematic nature of the Applicant's access requests amounts to an abuse of the right to make those requests.

[22] *In Request for Authorization to Disregard Access Requests – Grant MacEwan College* (March 13, 2007), the former Commissioner defined "abuse" to mean misuse or improper use. In that case, the Commissioner found that the applicant was not using the FOIP Act for the purpose for which it was intended, but as a weapon to harass and grind the College. He found that the applicant's requests were part of a long-standing history and pattern of behavior designed to harass, obstruct or wear the College down, which amounted to an abuse of the right to make those requests.

[1] Application by Alberta Municipal Affairs to disregard an access request made by an applicant under the *Freedom of Information and Protection of Privacy Act*. Available online at: https://www.oipc.ab.ca/media/134022/Section55_MunicipalAffairs_2002.pdf

[23] *In Request for Authorization to Disregard Access Requests – Alberta Justice and Solicitor General* (February 12, 2018), which I followed in *Request for Authorization to Disregard Access Requests – Alberta Health Services* (June 7, 2019) and in Request to Disregard F2019-RTD-03 (Calgary Police Service), I said that section 55(1)(a) of the FOIP Act clearly contemplates that the systematic nature of access requests, in and of themselves, may amount to an abuse of the right to make those access requests. I also said that section 55(1)(a) says nothing about an improper motive, although an improper motive would clearly establish abuse.

[24] I do not have any clear evidence that the purpose of the Applicant's access requests is to harass EPS or wear it down, although that is the effect of those access requests. Consequently, the issue I have to decide is whether there is something about the systematic nature of the Applicant's access requests that is a misuse or improper use of the FOIP Act.

[25] EPS stated:

> "… the Applicant has created false 911 calls for service. She has created counterfeit identities and fake check-on-welfare calls or other calls to her neighborhood; she has created fake Facebook accounts and posted messages on the SE Division Facebook page; has subsequently sent emails through to EPS members, as herself and as these other identities; and then FOIPPed the results of these communications."

[26] The Applicant did not address these allegations in her submission.

[27] These allegations are supported by both the evidence that EPS shared with the Applicant and the *in camera* information that I accepted.

[28] As was explained by EPS, the Applicant generates false calls for service and counterfeit identities and then continues to follow up on the results of these interactions with EPS by making numerous access requests. I am informed that the Applicant's pattern of access requests has resulted in 57 access requests to EPS since 2016, and in total, that she has made 68 FOIP requests to EPS over the past decade.

[29] The two access requests at issue, 2019-P-395 and P2019-P-396, are a part of this same pattern described by EPS, that being the Applicant's systematic monthly access requests for members' and EPS records. I am satisfied that the systematic nature of the Applicant's access requests regarding false calls for service and other apparent misrepresentations amounts to an abuse of the right to make those requests.

[30] The Applicant made submissions refuting an allegation that she designed malware. Nowhere in its submission does EPS claim the Applicant *designed* malware; rather, my understanding is that EPS' concern was with the Applicant's *inclusion* of malware in her

communications with EPS members regarding FOIP matters. In any event, given my above finding that the systematic nature of the Applicant's access requests amounts to an abuse of the right to make those requests, I do not find it necessary to consider EPS' concerns regarding malware. I also do not find it necessary to consider whether the requests are also frivolous or vexatious under section 55(1)(b) of FOIP.

Request for authorization to disregard future access requests

[31] EPS has requested authorization to disregard any future access requests that involve:

> *"…any and all information, regardless of format, relating to my name and/or address where I am listed in an EPS file #, and I did not call EPS for service"*
>
> *"…any and all information, regardless of format, regarding communication of any sort, in relation to my name and/or address that was received by/distributed by the following [named members].*

[32] EPS further requests a "cooling off" period of two years in which it does not have to respond to any FOIP requests from the Applicant.

[33] I have found that the systematic nature of the Applicant's access requests under the FOIP Act amounts to an abuse of the right to make those access requests. EPS's evidence is that the Applicant's pattern of conduct has been going on for a decade and has escalated since 2016. In my view, EPS has established that the Applicant's pattern of conduct is not going to change in the future unless there is some intervention. Therefore, I authorize EPS to disregard any future access requests from the Applicant of a similar type that EPS has set out above.

[34] However, given the quasi-constitutional nature of access rights, I am reluctant at this time to authorize EPS to disregard all access requests that the Applicant may make for the next two years.

[35] Nevertheless, if the Applicant continues to abuse her access rights, EPS may apply to me again under section 55(1) regarding any specific access or correction requests.

My decision

[36] I authorize EPS to disregard the Applicant's access requests 2019-P-395 and P2019-P-396 under section 55(1)(a) of the FOIP Act. I also authorize EPS to disregard future access requests of a similar type that EPS has set out above. However, at this time, I do not authorize EPS to disregard all access requests from the Applicant for the requested two year "cooling off" period.

Jill Clayton
Information and Privacy Commissioner