Information and Privacy Commissioner,
Ontario, Canada

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

ORDER MO-3477

Appeal MA16-138-2

Toronto Police Services Board

August 3, 2017

Summary: The appellants submitted an 11-part request to the police for records relating to cell site simulators. The police responded that no responsive records exist. During the inquiry into this appeal, the police provided representations to the effect that it is not possible to know whether responsive records exist because of difficulties with conducting an electronic search. The police argue that they conducted a reasonable search. They also rely on section 1 of Regulation 823, which excludes "machine-readable" records from the definition of "record" in section 2(1) where producing them would "unreasonably interfere" with operations. In this order, the adjudicator finds that the police did not conduct a reasonable search, and that section 1 of Regulation 823 does not apply. The police are ordered to conduct a new search for responsive records.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, as amended, section 1, 2(1) definition of "record," 17, 19, 20, 22 and 45; Regulation 823, sections 1 and 6.

Orders and Investigation Reports Considered: M-555, M-583, M-1123, MO-1488, MO-2003, MO-2863, P-50, P-81, P-1572, PO-2151, PO-2634, PO-2752, and PO-3373.

Cases Considered: *Toronto Police Services Board v. Ontario (Information and Privacy Commissioner)*, 2009 ONCA 20, 93 O.R. (3d) 563; *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27.

OVERVIEW:

[1] The appellants, two journalists, submitted an access request under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) to the Toronto Police Services Board (the police or the institution) for the following information:

1. Records regarding Toronto Police Services's acquisition of cell site simulators (also referred to as "IMSI catchers", "StingRay" devices, "DRTBox" devices or "KingFish" devices - "cell site simulators" below), including but not limited to invoices, purchase orders, contracts, loan agreements, evaluation agreements, solicitation letters, correspondence with companies and public agencies that provide the devices, and similar documents.

2. A copy of all meeting minutes for meetings pertaining to cell site simulators, IMSI catchers, "Stingray" devices, "DRTBox" devices or "KingFish" devices.

3. A copy of all memos or emails between TPS and [identified company].

4. A copy of all memos or emails between TPS and [identified company].

5. A copy of all memos or emails between TPS and [identified company].

6. A copy of all letters, agreements or other records containing guidelines or instructions for responding to Freedom of Information requests pertaining to [identified companies], cell site simulators, IMSI catchers, "Stingray" devices, "DRTBox" devices or "KingFish" devices.

7. Records regarding any offer, proposal, arrangement, agreement, or memorandum of understanding with Ontario Provincial Police, Royal Canadian Mounted Police, Canadian Security Intelligence Service, the Communications Security Establishment, the Department of National Defense, the Canadian Armed Forces, Canada Border Services Agency, Correctional Service Canada, or any agency or corporation in Canada, the United States, or elsewhere, to borrow, permanently acquire from, or use any cell site simulator owned or possessed by these organizations.

8. All nondisclosure agreements with [identified companies], any other corporation, and any provincial or federal agencies, regarding your agency's actual or potential possession or use of cell site simulators.

9. Records regarding policies and guidelines governing use of cell site simulators, including but not limited to:

    a. when, where and how they may be used

    b. logging, retention and purging of data from the devices

10. what kind of legal process (including an administrative warrant, judicial warrant, or other legal process) should or should not be obtained to use the devices.

11. Training materials for use of cell site simulators.

12. Any licenses, waivers, agreements or other records with federal or provincial communications regulatory agencies (e.g., Canadian Radio- television and Telecommunications Commission, etc.) concerning use of cell site simulators.

[2] The police did not respond within thirty days, and the appellants filed a deemed refusal appeal (MA16-138)[1] that was subsequently closed once the police had issued an access decision.

[3] The access decision stated that inquiries were made to members from Purchasing Services, Telecommunications Services, Intelligence Services and Legal Services. The results from those inquiries confirmed that records responsive to this request do not exist. The appellant filed an appeal of this decision with this office (the IPC) and a new appeal (MA16-138-2, which is the subject of this order) was opened.

[4] The appeal was assigned to a mediator under section 40 of the *Act*. Mediation did not resolve this appeal, which moved on to the adjudication stage of the appeal process, where an adjudicator conducts an inquiry under the *Act*. I began the inquiry by sending a Notice of Inquiry to the police, inviting them to provide representations, which they did. In their representations, the police claim that responsive emails would fall outside the scope of the definition of "record" in section 2(1) of the *Act*, based on a provision about "machine readable records" in Regulation 823. I therefore added this claim as an issue in the appeal.

[5] I then sent a Notice of Inquiry to the appellants, enclosing the complete representations of the police and inviting them to provide representations. Despite several follow-up contacts, the appellants did not provide representations.

[6] In this order, I conclude that the police did not conduct a reasonable search, and that section 1 of Regulation 823 does not apply. Accordingly, the order requires the police to conduct a further search for responsive records, and to issue a new access decision, either interim or final, to the appellants, treating the date of this order as the date of the request, and taking into account sections 17(2), 19, 20, 22 and 45 of the *Act*, and section 6 of Regulation 823.

---

[1] See section 22(4) of the *Act*.

DISCUSSION:

Did the police conduct a reasonable search for records? Do the records, if they exist, fall outside the definition of "record" because of section 1 of Regulation 823?

Introduction

[7] Where a requester claims that additional records exist beyond those identified by the institution, the issue to be decided is whether the institution has conducted a reasonable search for records as required by section 17.[2] If I am satisfied that the search carried out was reasonable in the circumstances, I will uphold the institution's decision. If I am not satisfied, I may order further searches.

[8] The *Act* does not require the institution to prove with absolute certainty that further records do not exist. However, the institution must provide sufficient evidence to show that it has made a reasonable effort to identify and locate responsive records.[3] To be responsive, a record must be "reasonably related" to the request.[4]

[9] A reasonable search is one in which an experienced employee knowledgeable in the subject matter of the request expends a reasonable effort to locate records which are reasonably related to the request.[5]

[10] A further search will be ordered if the institution does not provide sufficient evidence to demonstrate that it has made a reasonable effort to identify and locate all of the responsive records within its custody or control.[6]

[11] The police have provided combined representations on the issues of reasonable search and whether, based on section 1 of Regulation 823, responsive records that might exist would even qualify as "records."

[12] The latter issue arises under the definition of "record" in section 2(1) of the *Act*, and in particular, item (b) of the definition:

> "record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,
>
> (b) **subject to the regulations**, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other

---

[2] Orders P-85, P-221 and PO-1954-I.
[3] Orders P-624 and PO-2559.
[4] Order PO-2554.
[5] Orders M-909, PO-2469 and PO-2592.
[6] Order MO-2185.

> information storage equipment and technical expertise normally used by the institution; [Emphasis added.]

[13] Section 1 of Regulation 823 states:

> A record capable of being produced from machine readable records **is not included in the definition of "record"** for the purposes of the Act if the process of producing it would unreasonably interfere with the operations of an institution. [Emphasis added.]

[14] Although the police rely on this provision, they do not expressly argue that if it applies, the requested records would not be accessible under the *Act*. However, this is clearly the import of the section. Instead of taking that position, the police argue that it is impossible to know whether there are any responsive records because of the difficulties they have experienced in searching for them, and that accordingly, their search should be determined to be reasonable.

Representations

[15] In an affidavit provided with the police's representations, the Manager of Records Management Services indicates that the police's Access and Privacy Section (APS) sent an email to the Manager of Purchasing Services, requesting to confirm whether the following records existed, in reference to Mobile Device Identifiers (MDIs):

- Loan agreements;
- Contracts;
- Evaluation agreements;
- Solicitation letters;
- Correspondence with any companies and/or public agencies that
- manufacture/distribute and distribute the device; and,
- Any other similar documents.

[16] In a telephone call on the same day the email was sent, the Manager of Purchasing Services advised APS that no records exist.

[17] Following that, APS sent a further email to the Manager of Purchasing Services with inquiries as to whether their office had received any correspondence, specifically from the companies identified in items 3, 4 and 5 of the request. In response, the Manager of Purchasing Services confirmed that there were no purchase orders located for these three companies.

[18] The police subsequently issued a decision letter to the appellant, advising that records do not exist. As already noted, the access decision explained that "inquiries were made to members from Purchasing Services, Telecommunications Services, Intelligence Services and Legal Services. The results from those inquiries confirmed that records responsive to this request do not exist."

[19] After receiving the decision letter, the appellants appealed, and in their notice of appeal, they referred to a *Globe and Mail* article[7] to support their position that responsive records exist. The article suggests that an MDI had been used in connection with an investigation by the police.

[20] While the appeal was in the mediation stage, APS emailed two senior members of the police force, seeking assistance in dealing with the appeal. After two follow-up emails, it was "confirmed by Intelligence Services that the Toronto Police Service does not own a MDI, but has in the past utilized such a device for investigative purposes with the assistance of other investigative agencies."

[21] Subsequently, in connection with another request, APS contacted Information Security and requested "a complete search of the email system . . . specifically seeking all emails relating to MDIs." This search led to a re-evaluation of whether there might be responsive records in the present appeal. The affidavit of the police's Manager of Records Management Services explains this course of events:

> In processing [the request that led to this appeal ("this request")], the institution followed the established practice of liaising with the appropriate business stakeholders.[8] As the request did not involve searches of most commonly used police databases or systems, inquiries were directed to those business areas, thought to have greater knowledge of the purchase of equipment and the use of such a device. Based on the responses from those business areas, a decision letter was prepared for [this request]. IPC Orders P-24 and P0-2559 support that the Act does not require absolute certainty that records do not exist, but rather that sufficient evidence of reasonable efforts were made to respond.
>
> Subsequent to receiving [this request], another request . . . from yet another media agency was received by the institution also concerning MDIs - specifically, all emails referencing the device . . . . [T]he scope of [the new] request was very broad and required a departure from past practice of dealing with specific business areas. As a result, a search of the complete email system used by the TPS was required by the

---

7 https://www.theglobeandmail.com/news/national/case-involving-first-documented-use-of-stingray-technology-in-toronto-goes-to-trial/article30057813/.

8 From the police's access decision in this matter, I surmise that these stakeholders were the police's Purchasing Services, Telecommunications Services, Intelligence Services and Legal Services departments.

> institution. Searches using specific keywords within the mail files of the entire Service (just under 8000 members) yielded over 33,000 items or 36.9 Gigabytes of data.
>
> Although the institution was acting in good faith in its response to [this request], as a result of searches performed for [the new request] it was later determined that there might possibly be records relevant to [this request]. These requests have caused the institution to re-evaluate its processes and recognize where other methods may be more efficient in identifying records when the subject matter requires a corporate-wide search.
>
> However, due to the volume of results received, it is unknown the number of emails, if any, are directly relevant to [this request]. The results from the email search conducted by Information Security consist of both sent and received messages. Those mail messages are comprised of unsolicited messages, advertisements, news feeds, and could contain information for unrelated subjects possessing the same name (i.e. Stingray boat, Stingray fish, KingFish restaurant, etc.). There is no ability to limit the keyword search to MDI technology only. Furthermore, the substantial size of the search results significantly impacts the ability to browse mail content prompting a "Not Responding" system error whereby the computer is temporarily no longer operational.
>
> The above directly impacts the ability of an employee to open all mail files, folders and subfolders, and all attachments contained within those files, in order to review each message to determine responsiveness. If any message is identified as possibly responsive, further inquiries would be necessary to verify if those records were associated to any current ongoing police investigation or matters before the courts. If any responsive material is identified, an experienced member knowledgeable in the application of the MFIPPA would have to identify appropriate exemptions.

[22] On this basis, the police seek to invoke section 1 of Regulation 823, stating that "an undue burden would be placed on the institution to conduct the search because of the manner in which the records are organized and/or the manner in which the records would have to be retrieved."

[23] The police seek to support the argument that a search would be an undue burden by quoting the following passages from the Manager of Record Management Services' affidavit:

> As explained above, an undue burden would be placed on the institution because of the manner in which the records are organized and/or the manner in which the records would have to be retrieved.
>
> This institution received almost 6,000 requests in 2016, and compliance for the year was 55.9%. This compliance rate is far below the Toronto Police Services Board's compliance rate goal of 80% established on 2004.09.23 in Board Min, No. P284/04.
>
> The current challenge faced by the institution to meet the mandated 30-day response time has been previously addressed by Information Privacy Commissioner Brian Beamish in a letter dated May 22, 2015 to Toronto Police Chief Mark Saunders with a copy to then Toronto Police Services Board Chair Alok Mukhejee.
>
> Insufficient staffing levels within APS and the increasing number of requests continue to be an issue in the ability of the institution to meet the 30 calendar day compliance rate. This is further compounded by the complexity of the requests that are now being made. Such requests include unique record types which require more in-depth processing such as in-car camera, body-worn camera, media and statistical requests; all of which require the involvement of other business units such as Finance and Business Management, Strategy Management and other units within Operational Support Services. This issue is further exacerbated by the current 3-year hiring moratorium in the TPS, which has left little opportunity to expand the number of analysts to meet the ever increasing number of requests being received by the APS.
>
> The APS is presently staffed by 9 permanent Disclosures Analysts - 2 of which are currently on long term leave. Each analyst carries a caseload of approximately 250-300 open files; which does not include the almost 1,500 access requests past-compliance.

[24] In that regard, the police also rely on Order M-583, which they say stands for the proposition that "government organizations are not obliged to maintain records in such a manner as to accommodate the various ways in which a request for information might be framed."

Analysis

[25] I will begin my analysis by assessing whether the police have conducted a reasonable search. As the police themselves concede, they do not know whether responsive records might be produced by means of electronic searches, and based on the affidavit, I conclude that such searches have not been successfully completed.

[26] In the analysis below, I will address whether records that might be located

through electronic searching are excluded from the definition of "record" under section 1 of Regulation 823. However, assuming for the moment that such records are subject to the *Act*, I would conclude that in these circumstances, despite the other efforts undertaken, as described above, the police have not conducted a reasonable search. This was a comprehensive 11-part request, and the searches already conducted have produced no responsive records.[9]

[27] In that situation, I do not see how failing to follow an additional avenue (electronic searching) that might produce responsive records could result in the search being found to be "reasonable."

[28] Since electronic searches would produce "machine readable records," it is necessary at this point to consider section 1 of Regulation 823. To reiterate, this section states:

> A record capable of being produced from machine readable records is not included in the definition of "record" for the purposes of the Act if the process of producing it would unreasonably interfere with the operations of an institution.

[29] If this section applies, any responsive "machine readable records" that might be produced by electronic searching are not "records" within the meaning of the *Act*. Since the *Act* entitles requesters to ask for "records,"[10] "machine readable records" excluded from the definition under this section could not be requested under the *Act*, and I would not be able to order the police to conduct electronic searches for them.

[30] In Order P-50, Former Commissioner Sidney B. Linden addressed the parallel provision found in section 2 of Regulation 460, made under the provincial *Freedom of Information and Protection of Privacy Act*. He stated:

> What constitutes an "unreasonable interference" is a matter which must be considered on a case-by-case basis, but it is clear that the Regulation is intended to impose limits on the institution's responsibility to create a new record.

[31] In Order PO-3373, Senior Adjudicator Frank DeVries provided the following summary of previous decisions in this area:

> Orders since [Order P-50] have reviewed the various circumstances where this case-by-case analysis has been conducted. In Order PO-2752,

---

[9] In their representations, the police state that they located a template used in affidavits for legal authorization to use an MDI. The police have not issued an access decision concerning this document, which was given to the appellants with the police's representations during the inquiry. Even if it is responsive, its existence does not affect my analysis of the reasonable search issue.

[10] See section 4(1).

> Assistant Commissioner Brian Beamish reviewed a number of these orders and their findings. He also noted that these orders have confirmed that, in order to establish "interference," an institution must, at a minimum, provide evidence that responding to a request would "obstruct or hinder the range of effectiveness of the institution's activities."[11] These orders have also noted that, where an institution has allocated insufficient resources to the freedom of information access process, it may not be able to rely on "limited resources" as a basis for claiming interference.[12] Although government organizations are not obliged to maintain records in such a manner as to accommodate the various ways in which a request for information might be framed,[13] an institution must provide sufficient evidence beyond stating that extracting information would take "time and effort" in order to support a finding that the process of producing a record would unreasonably interfere with its operations.[14]

[32] Adjudicator Laurel Cropley also summarized prior decisions describing "unreasonable interference" in Order PO-2151:

> … in order to establish "interference", an institution must, at a minimum, provide evidence that responding to a request would "obstruct or hinder the range of effectiveness of the institution's activities" (Order M-850).
>
> While the size of the institution may be relevant to this issue, the availability of the fee provisions (and interim fee/access scheme), deposits and time extensions mitigate against a conclusion that an activity would interfere with the operations of the institution (Orders M-906, M-1071 and MO-1427).
>
> . . .
>
> In Order M-583, former Commissioner Tom Wright noted that, "government organizations are not obliged to maintain records in such a manner as to accommodate the various ways in which a request for information might be framed."
>
> Similarly, government organizations are not obligated to retain more staff than is required to meet its operational requirements. I qualify this point, however, by adding, as I noted above, that an institution must allocate

---

[11] Reference to Orders P-850 and PO-2151.
[12] Reference to Orders MO-1488 and PO-2151.
[13] Reference to Order M-583.
[14] Reference to Order MO-1989, upheld in *Toronto (City) Police Services Board v. Ontario (Information and Privacy Commissioner)*, [2009] O.J. No. 90 (C.A.); reversing [2007] O.J. No. 2442 (Div. Ct.).

sufficient resources to meet its freedom of information obligations (Order MO-1488).

[33] The position taken by the police is, essentially, that if a request would require an electronic search that would produce a significant number of "hits," causing a "'Not Responding' system error whereby the computer is temporarily no longer operational," this would "unreasonably interfere with the operations" of the police. No further specific evidence is given to show how such interference would occur; the police appear to take it as a given that the temporary unavailability of a computer automatically equals unreasonable interference.

[34] Specifically, the evidence provided by the police about the "system error" resulting from its attempted searches does not describe any actual interference with "the range of effectiveness" of the police's broader operations. I do not agree that the temporary disabling of a computer is, without more, confirmation of unreasonable interference.[15] Moreover, the evidence is not nearly as detailed or compelling as that which has previously resulted in findings of unreasonable interference; for example:

- Order P-1572, where senior technical and business personnel of the Ministry of Consumer and Commercial Relations would have required approximately 275 days to locate the information, diverting them from their normal core functions, and resulting in substantial human resources costs as well as 42 days of service interruption to all users of the Ministry's computerized registry of all business entities in Ontario;

- Order PO-2151, where producing a list of "authorized requesters" who had accessed the requester's personal information held by the Ministry of Transportation would occupy a significant amount of a senior analyst's time over a period of four weeks and developing a program to analyze the resulting data would require 375 days of programming and testing;

- Order PO-2752, where it would have taken staff at the Ministry of Correctional Services 1,377 hours to produce the de-identified contents of the ministry's offender tracking and information system, which would have diverted staff from working on "critical public safety business systems such as ... the police, courts and correctional services"; and

- Order PO-3373, which addressed a request similar to the one in Order PO-2151, and would have required 375 days of programming time to complete.

[35] The other evidence presented by the police pertains to "insufficient" staffing levels within APS, their problems meeting the 30-day time limit for responding to access

[15] See also Order MO-2003, where the adjudicator rejected an argument that searching would lead to the system "freezing," and that this would constitute unreasonable interference with operations.

requests mandated by section 19 of the *Act*, the complexity of other requests they now receive, and the fact that they are in the midst of a three-year hiring moratorium. Orders PO-2151 and MO-2863[16] affirm that "an institution must allocate sufficient resources to meet its freedom of information obligations." I agree. In my view, therefore, these arguments do not support a finding that the required electronic search for responsive records in this case would "unreasonably interfere" with the operations of the police.

[36] For all these reasons, I find that the police have not presented sufficient evidence to demonstrate that section 1 of Regulation 823 applies.

[37] I also note that the police do not refer to the time extension or fee provisions of the *Act*,[17] which exist, among other purposes, to alleviate the difficulty faced by institutions in processing onerous requests. These tools are augmented by the ability to issue an interim access decision and fee estimate as outlined in Orders P-81, M-555 and PO-2634, which apply "where the institution is experiencing a problem because a record is unduly expensive to produce for inspection by the head in making an access decision."[18] This leaves unanswered the question of whether the police could have taken other steps to facilitate their response to the request. There is also no evidence that they discussed these issues with the appellants to see whether the request could be broken down or reduced. Rather, they jettisoned the entire request by claiming that an electronic search is impossible, and/or an unreasonable interference with operations.

[38] Beyond the question of evidence, the argument advanced by the police also raises issues of statutory interpretation. In a world where email and electronic record-keeping are ubiquitous, the interpretation advanced by the police would have catastrophic consequences for access to information as it would mean that email and other electronic records could easily be excluded from the definition of "record," rendering them inaccessible under the *Act*.

[39] As noted by the Supreme Court of Canada, the modern approach to statutory interpretation requires the words of a provision to be read "in their entire context and according to their grammatical and ordinary sense, harmoniously with the scheme and

---

[16] See also Order MO-1488.

[17] See sections 20 and 45, and Adjudicator Cropley's summary of previous jurisprudence in Order PO-2151, quoted above, to the effect that "availability of the fee provisions (and interim fee/access scheme), deposits and time extensions mitigate against a conclusion that an activity would interfere with the operations of the institution.".

[18] The purpose for providing the option of an interim access decision is explained in Order M-1123: "The process outlined in Order 81 (and subsequently reviewed and confirmed in Order M-555) takes into account the interests and obligations of all parties. It allows the institution to determine an estimated fee from a position of knowledge; it gives the requester a basis for assessing the fee calculation, and also a preliminary indication of whether or not access will be granted; and it puts the Commissioner in a position to review the fee estimate should the requester appeal the institution's decision.".

object of the Act and the intention of the legislature".[19]

[40] The purposes of the *Act* are set out in section 1:

> The purposes of this Act are,
>
> (a) to provide a right of access to information under the control of institutions in accordance with the principles that,
>
> > (i) information should be available to the public,
> >
> > (ii) necessary exemptions from the right of access should be limited and specific, and
> >
> > (iii) decisions on the disclosure of information should be reviewed independently of the institution controlling the information; and
>
> (b) to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

[41] In *Toronto Police Services Board v. Ontario (Information and Privacy Commissioner)*,[20] the Ontario Court of Appeal upheld a decision of Senior Adjudicator Frank DeVries that also pertained to the interpretation of item (b) of the definition of "record" and section 1 of Regulation 823. On the question of statutory interpretation, the Court stated[21]:

> My third reason for concluding that the Adjudicator's decision on the s. 2(1)(b) issue is not unreasonable is that the principles of statutory interpretation and the requirement that the Act be given a fair, large and liberal construction support the decision he reached. As recently held by this court in City of Toronto Economic Development Corp. v. Ontario (Information and Privacy Commissioner), 2008 ONCA 366 (CanLII), [2008] O.J. No. 1799, 292 D.L.R. (4th) 706 (C.A.), at paras. 28 and 30, the Act should be given a broad interpretation to best ensure the attainment of its object, according to its true intent, meaning and spirit.
>
> In accordance with this approach, any question of statutory interpretation must begin with a consideration of the purpose and intent of the legislation. Here, s. 1 of the Act takes the mystery out of that exercise. In particular, s. 1(a) (i) and (ii) state that the purpose of the Act is to provide

---

[19] R. Sullivan, *Sullivan on the Construction of Statutes* (5th ed. 2008), at p. 1; *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27, at para. 21.
[20] 2009 ONCA 20, 93 O.R. (3d) 563.
[21] at paras. 43-48.

the public with a right of access to information under the control of municipal government institutions, in accordance with the principle that information should be made available subject only to limited and specified exemptions.

That approach -- one of presumptive access -- reflects the fact that, because municipal institutions function to serve the public, they ought in general to be open to public scrutiny. In this regard, I agree with the submissions of the intervenor that in enacting the Act, the legislature "wanted to improve the democratic process at the municipal and local board level" by ensuring members of the public would be able to access information needed "to participate in our democratic process in a worthwhile manner". As noted by the intervenor, the Act was advanced by the legislature as an "important step towards ensuring an open and very public operation of government at both the provincial and municipal levels": Ontario, Legislative Assembly, Official Reports of the Debates (Hansard), No. 49 (October 10, 1989) at 2772 (Mr. Elston).

Along these same lines, the Supreme Court of Canada has recognized that the overarching purpose of "access to information" legislation is to facilitate democracy. It does so in two ways -- first, it helps to ensure that citizens have the information required to participate meaningfully in the democratic process and second, it helps ensure that politicians and bureaucrats remain accountable to the citizenry: Dagg v. Canada (Minister of Finance), 1997 CanLII 358 (SCC), [1997] 2 S.C.R. 403, [1997] S.C.J. No. 63, at para. 61.

Dagg also teaches that members of the public cannot hope to hold the government to account without having adequate knowledge of what government institutions are doing; nor can they hope to participate in the decision-making process and contribute to the formation of policy and legislation if that process is hidden from view. It is fundamental to a healthy democracy that government processes be easily scrutinized by the very public the government is elected to serve. Transparency and accountability are vital to the democratic process: Dagg, at para. 61, citing Donald C. Rowat, "How Much Administrative Secrecy?" (1965) 31 Can. J. of Econ. and Pol. Sci. 479 at 480; see also Edmonton Journal v. Alberta (Attorney General), 1989 CanLII 20 (SCC), [1989] 2 S.C.R. 1326, [1989] S.C.J. No. 124, at p. 1373 S.C.R.

A contextual and purposive analysis of s. 2(1)(b) must also take into account the prevalence of computers in our society and their use by government institutions as the primary means by which records are kept and information is stored. This technological reality tells against an interpretation of s. 2(1)(b) that would

> **minimize rather than maximize the public's right of access to electronically recorded information**. [Emphasis added.]

[42] In my view, the approach advocated here by the police would minimize, rather than maximize, the public's right of access to electronically recorded information, and it must be rejected as antithetical to the purposes of the *Act*.

[43] For all these reasons, I find that the police did not conduct a reasonable search, and that section 1 of Regulation 823 does not apply.

Remedy

[44] I acknowledge that, as noted in Order M-583, government organizations are not obliged to maintain records so as to accommodate the various ways in which an access request could be framed. However, the inability to search electronic records for a term such as "stingray" without crashing the computer being used to do the search is untenable for an institution under the *Act* in the era of electronic record-keeping. [22]

[45] I have already noted that the police did not refer to various options that exist to assist institutions with onerous requests, such as time extensions, fees, and interim access decisions. As regards the method of searching, I have not been advised as to which email program or search software the police have used. While I note that item (b) in the definition of "record" refers to "software . . . normally used by the institution;" I would also point out that one possible category of fees set out in section 6 of Regulation 823 is, "for developing a computer program or other method of producing a record from machine readable record."

[46] I will order the police to conduct a further search for responsive records.

ORDER:

I order the police to conduct a further search for responsive records, and to issue a new access decision, either interim or final, to the appellants, treating the date of this order as the date of the request, and taking into account sections 17(2), 19, 20, 22 and 45 of the *Act*, and section 6 of Regulation 823.

---

[22] See also the comments of former Assistant Commissioner Mitchinson in his postscript to Order P-1572: "As the Ministry and other parts of government become increasingly reliant on electronic databases . . . to deliver their programs, it is critically important that public accessibility considerations be part of the decision-making process on any new systems design. . . . The public's statutory right of access to government records is a critically important component of our system of government accountability. Accessibility and transparency are inexorably linked to public trust and faith in government. Retaining access rights to raw electronic data is an important part of this overall accountability system, and factoring public access requirements into the design of new systems will ensure that these important rights are in fact enhanced rather than irretrievably lost through technology advances.".

Original Signed by: August 3, 2017

John Higgins
Adjudicator