Information and Privacy Commissioner,
Ontario, Canada

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

ORDER MO-4641

Appeal MA23-00597

Peel Regional Police Services Board

April 2, 2025

Summary: An individual made a request under the *Municipal Freedom of Information and Protection of Privacy Act* for records relating to the police's use of Clearview AI facial recognition technology.

The police granted partial access to records. The police withheld some information on the basis that disclosure would constitute an unjustified invasion of another individual's personal privacy (section 14(1)). The police also withheld other information on the basis that it was non-responsive to the request.

In this order, the adjudicator upholds the police's decision. She finds that the police properly withheld the information as either not responsive to the request or under the personal privacy exemption. She also finds that the public interest override (section 16) does not apply to permit its disclosure.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, as amended, sections 2(1) (definition of "personal information"), 14(1), 14(2)(a), 14(2)(f), 14(3)(b), 16, and 17.

Orders Considered: Orders MO-2019, MO-4403, MO-4459, MO-4269.

OVERVIEW:

[1] This order considers an individual's right of access under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) to information contained in records

relating to the Peel Regional Police Services Board's (the police) use of Clearview AI facial recognition technology.

[2] The requester originally made a request under the *Act* for access to all documents pertaining to the use of facial recognition technology by the police force and/or its members within a specific timeframe.

[3] The police issued a fee estimate which the requester (now the appellant) appealed to the Information and Privacy Commissioner of Ontario (IPC). This fee appeal was the subject of Order MO-4269.[1] The appellant subsequently paid the reduced fee.

[4] The police issued a final access decision in which they granted partial access to information relating to Clearview AI. The police denied access to some information, citing sections 12 (solicitor-client privilege) and 14(1) (personal privacy) of the *Act*. The police also withheld other information as it was considered non-responsive to the request.

[5] The appellant appealed the police's access decision to the IPC.

[6] During mediation, the appellant indicated that he was not seeking access to three legal memoranda that the police withheld pursuant to the solicitor-client exemption at section 12. Therefore, this information is no longer at issue in this appeal.[2] As for the remaining information withheld under the personal privacy exemption at section 14(1), the appellant raised the possible application of the public interest override at section 16.

[7] As mediation could not resolve this appeal, the file was transferred to the adjudication stage of the appeal process, where an adjudicator may conduct an inquiry under the *Act*. The adjudicator originally assigned to the appeal sought and received representations from the police and the appellant.

[8] The appeal was subsequently transferred to me to issue this decision.

[9] For the reasons that follow, I uphold the police's decision to withhold information identified as non-responsive. I also uphold the police's decision to withhold the personal information of affected parties pursuant to section 14(1) and find that the public interest override at section 16 does not apply in the circumstances. I dismiss the appeal.

RECORDS:

[10] The records remaining at issue consist of discussion notes, emails, cover pages,

[1] During mediation of the fee appeal, the appellant narrowed his request in an attempt to reduce the overall fee. The appellant also clarified that he was only seeking records relating to Clearview AI.

[2] In their representations, the police clarify that the section 12 exemption only applies to pages 16-24 and 730-738 of the records package. Based on my review of the records, these pages correspond with the legal memorandum that the appellant indicated he is no longer seeking access to. As a result, I find that the section 12 exemption is no longer at issue in this appeal and will not discuss it further in this order.

and literature, as set out in the following chart:

Description of Record	**Pages**	**Exemption**
Discussion notes	62 (withheld in part), 63-64, 280 (withheld in part), 281-282, 331 (withheld in part), and 332-333	Non-responsive
Internal emails and correspondence relating to other FOI request	132-133, 139-140, 201-203, 258-259, 287-288, 349-350, 413-414, 419-420, 497-500, 641-643, and 762	Non-responsive
Other emails	146-149, 252, 278 (withheld in part), and 435-442	Non-responsive
	207 (withheld in part), 210 (withheld in part), 215 (withheld in part), 225 (withheld in part), 228 (withheld in part), 233 (withheld in part), 237 (withheld in part), 240 (withheld in part), 267 (withheld in part), 268 (withheld in part), 275 (withheld in part), 362 (withheld in part), 382 (withheld in part), and 492 (withheld in part)	Section 14(1)
Cover pages	204 (withheld in part), 260 (withheld in part), 276 (withheld in part), 289 (withheld in part), 354 (withheld in part), 370 (withheld in part), 380 (withheld in part), 391 (withheld in part), 403 (withheld in part), and 417-418	Non-responsive or section 14(1)
Clearview AI Literature	747 and 750-757	Section 14(1)

ISSUES:

A. What is the scope of the request? What information is responsive to the request?

B. Do the records contain "personal information" as defined in section 2(1) and if so, whose personal information is it?

C. Does the mandatory personal privacy exemption at section 14(1) apply to the information at issue?

D. Pursuant to section 16, is there a compelling public interest in the disclosure of the records?

DISCUSSION:

Issue A: What is the scope of the request? What information is responsive to the request?

[11] The police withheld information from discussion notes as well as internal emails and correspondence on the grounds that they were non-responsive to the appellant's request. The police also indicated that information from cover pages, which precede and organize attached police records, were withheld as non-responsive to the request or alternatively, under the personal privacy exemption at section 14(1).

[12] Section 17 of the *Act* imposes certain obligations on requesters and institutions when submitting and responding to requests for access to records. This section states, in part:

> (1) A person seeking access to a record shall,
>
> > (a) make a request in writing to the institution that the person believes has custody or control of the record, and specify that the request is being made under this Act;
> >
> > (b) provide sufficient detail to enable an experienced employee of the institution, upon a reasonable effort, to identify the record;
>
> . . .
>
> (2) If the request does not sufficiently describe the record sought, the institution shall inform the applicant of the defect and shall offer assistance in reformulating the request so as to comply with subsection (1).

[13] To be considered responsive to the request, records must "reasonably relate" to the request.[3] Institutions should interpret requests liberally, to best serve the purpose and spirit of the *Act*. Generally, any ambiguity in the request should be resolved in the requester's favour.[4]

[3] Orders P-880 and PO-2661.
[4] Orders P-134 and P-880.

Representations

[14] The police indicate that they withheld portions of discussion notes as non-responsive to the request.[5] The police submit that it is evident from a review of the sender and the contents that this information does not pertain to the "use of facial recognition technology by the police force and/or any of its members".

[15] The police also indicate that some of the internal emails and correspondence included in the records package are not responsive to the request. The police submit that these pages relate to another request and should not have been included in the records package relating to the appellant's request.[6]

[16] The police explain that they received two similar requests from two separate individuals (i.e. the appellant and an unrelated individual), and that they intended to leverage the work that they had completed in responding to the other individual's request for the purposes of responding to the appellant's request.

[17] However, the police indicate that pages which were solely responsive to the other individual's request were then included by error in the records package destined for the appellant. These pages were also mistakenly referred to in the index of records produced in response to the appellant's request and identified as being subject to an exemption.[7] The police explain that the exemption was applied in the context of the other request and reproduced by mistake in the index of records for this request. The police submit that these pages were clearly included in error because they contain the name and file number associated with the other requester and request.

[18] The police also indicate that other internal emails and correspondence, while not related to the other request, nevertheless contain information that is non-responsive to this request.[8] For instance, the police submit that pages 435-442 are about an entirely different matter.

[19] Finally, the police submit that the cover pages to attachments also contain information that is not responsive to the request.[9] While the police granted the appellant access to the attachments that were responsive to his request, the cover pages to these attachments were initially compiled in response to the other individual's request and therefore contain references to that other individual. The police submit that this information was withheld as non-responsive to the appellant's request or alternatively, under the personal information exemption at section 14(1) of the *Act*.

---

[5] Pages 62 (withheld in part), 63-64, 280 (withheld in part), 281-292, and 331 (withheld in part).
[6] Pages 132-133, 139-140, 201-203, 258-259, 287-288, 349-350, 413-414, 419-420, 497-500, 641-643, and 762.
[7] Specifically, the index stated that some of these records were withheld pursuant to section 12 and others as non-responsive.
[8] Pages 146-149, 252, 278 (withheld in part), and 435-442.
[9] Pages 204, 260, 276, 289, 354, 370, 380, 391, and 403, all withheld in part, and pages 417-418.

[20] The appellant submits that if the records were truly unrelated to the request, the police would not have identified them or included them in the index of records. The appellant submits that the inclusion of the records in the index, which was prepared solely by the police, is an acknowledgement of their relevance and supports the conclusion that these records are responsive.

Analysis and findings

[21] I have reviewed the records and find that the withheld information from discussion notes, internal emails and correspondence, as well as cover pages of attachments is non-responsive to the appellant's request.

[22] I agree with the police's assessment that the withheld portions of the discussion notes do not relate to the "use of facial recognition technology by the police force and/or any of its members" and therefore are not reasonably related to the appellant's request. My review of the list of discussion topics, which the appellant received as part of the discussion notes, supports the conclusion that the withheld information relates to topics that are not responsive to the appellant's request.

[23] I have also reviewed the internal emails and correspondence, which the police submit should not have been included in the package to the appellant because they are responsive to another request and not responsive to the appellant's request. I accept that these emails and correspondence contain explicit references to the name and file number associated with the other requester and are about searches that were conducted in relation to that other request. Considering the contents of these emails and correspondence, I also accept the police's explanation that they were mistakenly included in the records package to the appellant as a result of an administrative error.

[24] I further find that the police properly withheld information from other internal emails and correspondence as non-responsive to the appellant's request. Based on my review of the records, I am satisfied that this information is not responsive to the appellant's narrowed request, has no apparent relation to the appellant's request at all, or appears in the context of a record that also contains responsive information, which the police has disclosed in part.

[25] I am not convinced that the inclusion of a record in an index of records is determinative of its responsiveness. While I understand the appellant to be making a point about the reliability of the police's index of records, the police provided an explanation for how non-responsive records were accidentally included in the records package and index. Given the significant number of records that were identified and reviewed in response to this request, I find that the police's explanation of its errors, while unfortunate, is plausible and I accept it. Additionally, I note that where a record contains both responsive and non-responsive information (as seen in this appeal), the presence of this non-responsive information would also be reflected in the index of records.

[26] Finally, I accept that the information that was withheld from the cover pages concerns the other request and is therefore non-responsive to this request. In addition to these cover pages, which were withheld in part, the police also withheld an additional cover page and its corresponding attachment in full. I have reviewed these pages and find that they are also non-responsive to the appellant's request. From my review, I accept that these pages were prepared upon receipt of the other request and similarly contain information regarding the police's response to that other request which is non-responsive to the appellant's request.

[27] In conclusion, I uphold the police's decision to withhold information from discussion notes, internal emails and correspondence, and cover pages on the basis that it is non-responsive to the appellant's request.

Issue B: Do the records contain "personal information" as defined in section 2(1) and if so, whose personal information is it?

[28] The police rely on the mandatory personal privacy exemption at section 14(1) of the *Act* to deny access to portions of the records. Before I consider whether this exemption applies, I must first determine whether the records contain "personal information". If they do, I must determine whether the personal information belongs to the appellant, to other identifiable individuals, or both.

[29] It is important to know whose personal information is in the records. If the records contain the requester's own personal information, their access rights are greater than if they do not.[10] Also, if the records contain the personal information of other individuals, one of the personal privacy exemptions might apply.[11]

[30] Section 2(1) of the *Act* defines "personal information" as "recorded information about an identifiable individual". Recorded information is information recorded in any form, including paper and electronic records.[12]

[31] Information is "about" an individual when it refers to them in their personal capacity, meaning that it reveals something of a personal nature about that individual. Information is about an "identifiable individual" if it is reasonable to expect that an individual can be identified from the information either by itself or if combined with other information.[13]

[32] Section 2(1) of the *Act* contains some examples of personal information[14], though

---

[10] Under sections 36(1) and 38 of the *Act,* a requester has a right of access to their own personal information, and any exemptions from that right are discretionary, meaning that the institution can still choose to disclose the information even if the exemption applies.
[11] See sections 14(1) and 38(b).
[12] See the definition of "record" in section 2(1) of the Act.
[13] Order PO-1880, upheld on judicial review in Ontario (Attorney General) v. Pascoe, [2002] O.J. No. 4300 (C.A.).
[14] Specifically paragraphs (a) to (h) of the definition of personal information at section 2(1).

this list is not exhaustive. Therefore, information that does not fall under paragraphs (a) to (h) may still qualify as personal information.

Representations

[33] The police submit that the records contain the personal information of other individuals (affected parties), but not the appellant. The police submit that it is reasonable to expect that these affected parties may be identified from the information in the records, which includes personal identifiers such as name, age, sex, race, information relating to criminal and/or employment history, identifying markers, identifying images, phone numbers, physical addresses, and personal email addresses. The police indicate that in rare cases where information sent from a professional email address has been redacted pursuant to section 14(1) of the *Act*, this is because the information was entirely personal in nature.

[34] The appellant does not make any specific submissions with respect to the personal information at issue, other than to state that there is no justification for the "wholesale" withholding of records relating to the police's use of the Clearview AI software as any personal information can be severed from the records.

Analysis and findings

[35] The police identified and withheld portions of emails[15], as well as several pages of Clearview AI "literature"[16] as personal information. I have reviewed these records and agree that they contain information that qualifies as the personal information of other individuals and do not contain the appellant's personal information.

[36] Based on my review of the records, the emails include a range of correspondence between service members and internal and external parties. While most of these emails contain information about setting up and troubleshooting a Clearview AI software trial, another email (which is duplicated in the records package) contains a summary of a service member's use of the software trial. I find that these emails contain personal information as defined in section 2(1) of the *Act*, including the personal email addresses of service members, the personal telephone numbers of a service member and another identifiable individual, the personal IP address of a service member, details about a service member's personal schedule, and an affected party's name. To be clear, this is the only information that the police withheld from the emails; the remainder of the email contents were disclosed to the appellant.

[37] The Clearview AI literature contains investigative summaries and examples of Clearview AI use in other jurisdictions. This information appears to have been compiled by Clearview AI in the form of a slide deck and presented to the police, possibly for promotional purposes. I find that the Clearview AI literature also contains information

[15] Portions of pages 207, 210, 215, 225, 228, 233, 237, 240, 267, 268, 275, 362, 382, and 492.
[16] Pages 747 and 750-757.

that qualifies as personal information as defined in section 2(1), including information relating to the race, national or ethnic origin, colour, age, or sex of an individual, information relating to the criminal history of an individual, addresses, individuals' names, along with other personal information relating to them, and photographs.

[38] The appellant submits that the police should redact any personal information from the records and disclose the remaining information that is responsive to his request. The police dispute the appellant's characterization of their redactions as "wholesale". They argue that the redactions from the emails were limited to only the personal information of affected parties, while the remainder of the information in the emails was disclosed. The police further indicate that only 9 out of 840 total pages, consisting of Clearview AI literature, were withheld in full for containing the personal information of identifiable individuals.

[39] I have considered whether the personal information of the affected parties can be severed from the records in such a way that would allow additional information to be disclosed. I have reviewed the emails and agree that the redactions to those are minimal and limited to the personal information of affected parties. Based on my review of the Clearview AI literature, I conclude that the personal information of the affected parties and any other information in those records is so intertwined such that additional severances are not feasible.

[40] Having found that the records contain the personal information of other individuals, I will consider whether the personal information is exempt from disclosure under the mandatory personal privacy exemption at section 14(1) of the *Act*.

Issue C: Does the mandatory personal privacy exemption at section 14(1) apply to the information at issue?

[41] One of the purposes of the *Act* is to protect the privacy of individuals with respect to their own personal information held by institutions. Section 14(1) of the *Act* creates a general rule prohibiting an institution from disclosing personal information about another individual to a requester. This general rule is subject to a number of exceptions.

[42] The section 14(1)(a) through (e) exceptions are relatively straightforward. If any of these exceptions apply, the institution must disclose the information. Neither the police nor the appellant claim that any of the exceptions at sections 14(1)(a) through (e) apply in the circumstances of this appeal and I am satisfied that none apply.

[43] The section 14(1)(f) exception is more complicated. It requires the institution to disclose another individual's personal information to a requester only if this would not be an "unjustified invasion of personal privacy". Other parts of section 14 must be looked at to decide whether disclosure of the other individual's personal information would be an unjustified invasion of personal privacy.

[44] Sections 14(2), (3), and (4) help in deciding whether disclosure would or would

not be an unjustified invasion of personal privacy. Section 14(3) should generally be considered first.[17] This section outlines several situations in which disclosing personal information is presumed to be an unjustified invasion of personal privacy.

[45] If one of the presumptions in section 14(3) applies, the personal information cannot be disclosed unless:

- there is a reason under section 14(4) that disclosure of the information would **not** be an "unjustified invasion of personal privacy," or
- there is a "compelling public interest" under section 16 that means the information should nonetheless be disclosed (the "public interest override").[18]

[46] If the personal information requested does not fit within any presumptions under section 14(3), one must consider the factors set out in section 14(2) to determine whether disclosure would be an unjustified invasion of personal privacy.

Representations

[47] The police submit that the information in the records was compiled as part of an investigation into a possible violation of law, engaging the presumption at section 14(3)(b). The police submit that the information was captured by various police services while conducting criminal investigations under federal statutes. The police indicate that while they are not the investigating agency and therefore not in a position to comment on the status of any proceedings, all of the allegations were criminal in nature.

[48] The police further submit that none of the section 14(4) limitations apply. However, in case the presumption at section 14(3)(b) is found not to apply, the police state that several factors under section 14(2) apply and weigh against disclosure.

[49] First, the police submit that the information withheld from the emails and the Clearview AI literature is highly sensitive within the meaning of section 14(2)(f). With respect to the personal information in the emails, the police argue that service members have a considerable interest in keeping their personal contact information private, particularly given their public-facing role. The police also indicate that they withheld nine pages of Clearview AI literature containing personal information belonging to affected parties, some of whom were the subject of police investigations in multiple jurisdictions. The police submit that the disclosure of this personal information could result in significant personal distress.

[50] The police explain that because they did not compile most of the personal information in the records, they cannot guarantee its accuracy or reliability (section

---

[17] If any of the section 14(3) presumptions are found to apply, they cannot be rebutted by the factors in section 14(2) for the purposes of deciding whether the section 14(1) exemption has been established.
[18] *John Doe v. Ontario* (*Information and Privacy Commissioner*) (1993), 13 O.R. (3d) 767 (Div.Ct.).

14(2)(g)). Furthermore, given the highly sensitive nature of the information, the police suggest that it is possible that disclosure will unfairly damage the reputation of the individuals named in the records (section 14(2)(i)). The police also submit that the personal information was supplied to them in confidence (section 14(2)(h)). All of these factors, they submit, weigh against disclosure.

[51] The police submit that the only factor that may weigh in favour of disclosure would be to subject the activities of the institution to public scrutiny under section 14(2)(a). However, the police argue that this factor should be given limited weight considering: the police only ever possessed a "demo" version of the software in question, the software was never used in any active investigations, and use of the software ceased entirely as of January 27, 2020.

[52] The appellant does not provide substantive representations on whether any of the sections 14(1)(a) through (f) exceptions apply, or on whether disclosure would constitute an unjustified invasion of personal privacy pursuant to sections 14(2), (3), and (4). However, the appellant reiterates that there is no justification for withholding the records in their entirety, as any personal information can be severed.

Analysis and findings

Section 14(3)(b) presumption

[53] The presumption against disclosure at section 14(3)(b) states:

> A disclosure of personal information is presumed to constitute an unjustified violation of personal privacy if the personal information,
>
> > was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation[.]

[54] Based on my review of the records, the police withheld personal information from two categories of records – emails and Clearview AI literature – on the grounds that this information was compiled and is identifiable as part of an investigation into a possible violation of law.

[55] While I agree with the police's description of the withheld information as being identifiable personal information, I am not convinced that the emails were compiled as part of an investigation into a possible violation of law. In their representations, the police indicate that most of the personal information in the emails was provided in the context of setting up a software trial. I am unable to see how information about setting up and troubleshooting a Clearview AI software trial falls within the circumstances contemplated by section 14(3)(b). Similarly, I have not received any evidence about how the personal information at issue (which consists of personal email addresses, personal telephone numbers, a personal IP address, details about a service member's personal schedule, and

an affected party's name) relates to an investigation or what the alleged violation of law might be. As a result, I find that the section 14(3)(b) presumption does not apply to the personal information in the emails.

[56] Regarding the Clearview AI literature, the police submit that it contains the personal information of affected parties, which was captured by various police services in the course of criminal investigations. The police refer to this information as "investigative summaries". These summaries contain descriptions of various incidents, along with details about the investigation and the outcome.

[57] Previous IPC orders have found that summaries of police investigations, created after the investigation, are not investigatory in nature and "are clearly not for use in any particular investigation [or] compiled as part of any specific investigation".[19] I agree with and adopt this reasoning.

[58] In this case, most of the descriptions in the literature include information about the outcome of an investigation. In my view, this supports the conclusion that these records were created after the investigation, and not as part of it. Furthermore, it is my understanding that the information in the records was compiled by Clearview, and not by the police or any of the investigating agencies. In doing so, Clearview appears to be describing investigations which were conducted by other agencies, and which incorporated the use of Clearview AI, rather than conducting its own investigations. This information was then presented to the police, possibly for promotional or informational purposes. For these reasons, I am not convinced that the personal information in the Clearview AI literature was compiled as part of any specific investigation. Therefore, I find that the section 14(3)(b) presumption does not apply to the personal information in the literature.

Section 14(2)(a): Public scrutiny

[59] As none of the presumptions in section 14(3) apply, I will consider whether any of the section 14(2) factors apply.

[60] The police submit that the sections 14(2)(f), 14(2)(g), 14(2)(h), and 14(2)(i) factors apply and weigh against disclosure. While the police acknowledge that the section 14(2)(a) factor may be relevant, they argue that it carries little weight.

[61] The appellant has not made submissions on whether section 14(2)(a) or any other factor applies in favor of disclosure.

[62] Section 14(2)(a) promotes transparency of government action and supports disclosure where it would subject the activities of the government to public scrutiny.[20] An institution should consider the broader interests of public accountability when considering

[19] Order MO-2019. See also Orders MO-4403 and MO-4459.
[20] Order P-1134.

whether disclosure is "desirable" or appropriate to allow for public scrutiny of its activities.[21]

[63] I find that disclosure of the personal information in the emails would not promote transparency of government action in the manner contemplated by section 14(2)(a). The amount of personal information that the police withheld from these records is already extremely limited. The redacted email addresses, phone numbers, and other personal information have no obvious relation to the activities of government and their disclosure is unlikely to reveal anything of substance about the police's activities, particularly considering the email contents which have already been disclosed to the appellant. I am not convinced that disclosure of the personal information in the emails is relevant to, or desirable for, public scrutiny. I conclude for these reasons that the section 14(2)(a) factor does not apply to this information.

[64] I acknowledge that the police's use or potential use of facial recognition technology is a matter of public interest. Both the former and current Commissioners, as well as their federal, provincial, and territorial (FPT) counterparts, have recognized that facial recognition technologies, including Clearview AI, carry significant privacy implications for Ontarians.[22] Previous adjudicators have similarly recognized the importance of contributing to ongoing public debates about the use of facial recognition technologies by law enforcement.[23]

[65] However, in order for section 14(2)(a) to apply, it is necessary to evaluate whether the disclosure of the specific personal information at issue would be "desirable for the purpose of subjecting the activities of the institution to public scrutiny". While the above references demonstrate that "facial recognition technology" as a subject matter has been recognized as a matter of public interest, section 14(2)(a) requires a further inquiry into the nature of the personal information at issue and the possible effects of its disclosure.

[66] In this case, despite the public interest in the overarching subject matter of the request (i.e. information related the police's use of Clearview AI), I find that there is insufficient evidence for me to conclude that disclosure of the personal information of individuals captured in the Clearview AI literature would promote transparency of government action or subject the activities of the police to public scrutiny. Specifically, given my finding that the police were not the investigating agency and did not compile the personal information in the Clearview AI literature, it is unclear how this information bears any relation to the police's activities. Although the police appear to have received and reviewed this information provided by Clearview AI, possibly for promotional or informational purposes, I am not convinced that the information at issue reveals anything

---

[21] Order P-256.
[22] "Recommended legal framework for police agencies' use of facial recognition, Joint Statement by Federal, Provincial and Territorial Privacy Commissioners", (2 May 2022), online: www.priv.gc.ca. See also, Brian Beamish, "Statement on Toronto Police Service Use of Clearview AI Technology", Information and Privacy Commissioner of Ontario (14 February 2020), online: www.ipc.on.ca.
[23] Order MO-4269.

about the police's activities or the activities of any other provincial or regional police agency.

[67] In my view, there is insufficient connection between the personal information at issue, which appears to concern affected parties and incidents that fall solidly outside the police's jurisdiction, and the activities of the institution itself. As disclosure would not fulfill the purpose of subjecting the actions of the police to public scrutiny, I conclude that the factor at section 14(2)(a) does not apply to the personal information in the literature.

Section 14(2)(f): Highly sensitive

[68] Section 14(2)(f) is intended to weigh against disclosure when the evidence shows that the personal information is highly sensitive. To be "highly sensitive", there must be a reasonable expectation of significant personal distress if the information is disclosed.[24]

[69] The police claim that section 14(2)(f) applies to the personal information at issue. As previously indicated, this includes the personal information of service members and other affected parties in emails, as well as the personal information captured in the Clearview AI literature relating to the age, sex, race, national or ethnic origin, and criminal history of affected parties, along with other personal information relating to them, including their photographs.

[70] I accept that this information is highly sensitive. Specifically, I am satisfied that the personal information in the emails, which includes the personal contact information of service members and another affected party, the personal IP address of a service member, details about a service member's personal schedule, and an affected party's name, is of an inherently sensitive nature. I agree with the police that service members who regularly interact with members of the public have an interest in maintaining the privacy of their personal information for safety and security reasons, and that the disclosure of this information could reasonably be expected to cause them significant personal distress.

[71] With respect to the Clearview AI literature, I have considered the nature and quantity of the personal information at issue, the circumstances which necessitated police involvement, and the serious-yet-unverified nature of the allegations being made. Given these circumstances, I find that disclosure of this information could reasonably be expected to cause the affected parties significant personal distress.

[72] As a result, I find that the personal information at issue is highly sensitive and the factor at section 14(2)(f) applies, weighing against disclosure.

Balancing the relevant factors

[73] I have found that the section 14(2)(a) factor in favour of disclosure does not apply,

[24] Orders PO-2518, PO-2617, MO-2262 and MO-2344.

while the section 14(2)(f) factor applies and weighs against disclosure. Having found one factor weighing against disclosure and no factors weighing in favour of it, it is not necessary for me to consider the other factors at sections 14(2)(g), 14(2)(h), and 14(2)(i), which would weigh further against disclosure if found to apply.

[74] As a result, I uphold the police's decision to deny access to the personal information in the emails and Clearview AI literature pursuant to the mandatory personal privacy exemption at section 14(1) of the *Act*.

Issue D: Pursuant to section 16, is there a compelling public interest in the disclosure of the records?

[75] Section 16 of the *Act*, the "public interest override", provides for the disclosure of records that would otherwise be exempt under another section of the *Act*.

[76] Section 16 states:

> An exemption from disclosure of a record under sections 7, 9, 9.1, 10, 11, 13 and **14** does not apply if a compelling public interest in the disclosure of the record clearly outweighs the purpose of the exemption.

[77] For section 16 to apply, two requirements must be met. First, there must be a compelling public interest in the disclosure of the records. Second, this interest must clearly outweigh the purpose of the exemption.

[78] Section 16 can only apply to information withheld pursuant to a number of specified exemptions. In this case, I will consider whether the public interest override applies to the information that the police withheld pursuant to section 14(1).

The police's representations

[79] The police submit that there is no compelling public interest in disclosure of the personal information that has been withheld from the records that overrides the section 14(1) exemption. The police indicate that the Office of the Information and Privacy Commissioner of Canada (OPC) has conducted a review of Clearview AI's facial recognition program, as well as the use of facial recognition technology by law enforcement agencies more generally, and therefore the subject matter has already been effectively dealt with. The police suggest that the program is no longer an active concern, particularly because Clearview AI is no longer operating within Canada. The police also restate the arguments that they made regarding the section 14(2)(a) factor and submit that they apply here.

[80] The police further submit that the majority of the responsive information in the emails and Clearview AI literature has already been disclosed to the appellant. The police submit that they applied limited redactions to protect the personal privacy of various affected parties, and that disclosure of this information would not serve the public

interest. The police submit that this issue has already received wide public coverage and debate, and disclosing the information they withheld under section 14(1) would not shed any further light on the subject.

The appellant's representations

[81] The appellant submits that there is a significant public interest in disclosure of the information that has been withheld. The appellant indicates that he is an academic researcher who is conducting a case study on the use of Clearview AI by police forces in southern Ontario. The appellant states that he is under advance contract with a publisher and that the results of the case study will be included in his upcoming book.

[82] Contrary to the police's claims, the appellant suggests that since the initial and limited journalistic interest in the police's use of the technology in 2020, there has been virtually no sustained public discussion or dissemination of information on this subject. More specifically, the appellant claims that there has been almost no published discussion about the use of Clearview AI by the respondent police board and other police agencies across the country.

[83] As an example, the appellant cites a recent book on Clearview AI which identifies various Ontario regional police services as heavy users of the technology, but does not elaborate on their actual use. The appellant submits that accessing the records will allow him to contribute a more holistic, balanced, and localized perspective about the topic, especially with his intended focus on regional police services in Ontario.

Analysis and findings

[84] The *Act* is silent as to who bears the burden of proof in respect of section 16. This onus cannot be completely borne by an appellant, who has not had the benefit of reviewing the requested records before making submissions. To find otherwise would be to impose an onus which could seldom if ever be met by an appellant. Accordingly, the IPC will generally review the records with a view to determining whether there could be a compelling public interest in disclosure that clearly outweighs the purpose of the exemption.[25]

[85] In considering whether there is a "public interest" in disclosure of the record, the first question to ask is whether there is a relationship between the record and the *Act*'s central purpose of shedding light on the operations of government.[26] In previous orders, the IPC has stated that in order to find a compelling public interest in disclosure, the information in the record must serve the purpose of informing or enlightening the citizenry about the activities of their government or its agencies, adding in some way to the information the public has to make effective use of the means of expressing public

[25] Order P-244.
[26] Orders P-984 and PO-2607.

opinion or to make political choices.[27]

[86] The IPC has defined the word "compelling" as "rousing strong interest or attention".[28] The IPC must also consider any public interest in **not** disclosing the record.[29] A public interest in the non-disclosure of the record may bring the public interest in disclosure below the threshold of "compelling."[30]

[87] I accept that the use or potential use of facial recognition technology by police agencies is a matter of public interest. I find support for this in the guidance materials that the federal, provincial, and territorial (FPT) privacy commissioners have developed for police agencies on the use of facial recognition technology[31], as well as specific guidance that this office developed for Ontario police on the use of facial recognition technology in connection with mugshot databases[32].

[88] In the latter guidance document, the IPC recognizes that "the technology raises significant legal, privacy, and ethical challenges given its potential to provide biased or inaccurate results and undermine rights and freedoms" and describes concerns raised by members of the public, civil society, government, and academia.[33] The IPC reiterates concerns raised in the joint FPT guidance about inappropriate uses of facial recognition technology that may have "lasting and severe effects on privacy and other fundamental rights" and renews the call "for collective reflection on the limits of acceptable [facial recognition] use".[34]

[89] I accept that the use of Clearview AI by various police agencies is a matter of public interest. In their representations, the police reference a joint investigation into Clearview AI by the OPC, the Commission d'accès à l'information du Québec (CAI), the Information and Privacy Commissioner for British Columbia (OIPC BC), and the Information and Privacy Commissioner of Alberta (OIPC AB).[35] The investigation identifies concerns with Clearview's information practices and makes several recommendations and orders, including that Clearview cease offering facial recognition services to clients in

---

[27] Orders P-984 and PO-2556.
[28] Order P-984.
[29] *Ontario Hydro v. Mitchinson,* [1996] O.J. No. 4636 (Div. Ct.).
[30] Orders PO-2072-F, PO-2098-R and PO-3197.
[31] "Privacy guidance on facial recognition for police agencies", Office of the Privacy Commissioner of Canada (2 May 2022), online: www.priv.gc.ca.
[32] "Facial Recognition and Mugshot Databases: Guidance for Police in Ontario", Information and Privacy Commissioner of Ontario (1 February 2024), online: www.ipc.on.ca.
[33] *Ibid*.
[34] "Privacy guidance on facial recognition for police agencies", *supra* note 31.
[35] "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta", Office of the Privacy Commissioner of Canada (2 February 2021), online: www.priv.gc.ca. A judicial review application by Clearview AI against the decision of OIPC BC was recently dismissed by the Supreme Court of British Columbia, in *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, 2024 BCSC 2311.

Canada.

[90] Although I have found that the police's use or potential use of facial recognition technology and/or Clearview AI are matters of public interest, this does not necessarily mean that there is a compelling public interest in the disclosure of the specific personal information that remains at issue. For reasons similar to why I found that the disclosure of the affected parties' personal information is not relevant to or desirable for the purpose of subjecting the activities of the institution to public scrutiny (section 14(2)(a)), I find that the public interest override at section 16 does not apply.

[91] Disclosure of the personal information at issue, which includes personal contact information, as well as information relating to age, sex, race, national or ethnic origin, criminal history, photographs, and other personal information, does not appear to serve the purpose of shedding light on the operations of government. In my view, the appellant has not adequately explained how receiving the personal information of affected parties (in addition to the general information that has already been disclosed to him in large part) would improve his understanding of the police's operations. While I understand that the appellant is interested in the use of Clearview AI by regional police services in Ontario, the personal information at issue does not bear any relation to the activities of the respondent police. The fact that the police were not the investigating agency and did not compile the information at issue makes any connection even more tenuous.

[92] Even if I were to accept that there was a compelling public interest in the disclosure of the information at issue, I am not convinced that this interest clearly outweighs the purpose of the section 14(1) exemption in this case. I previously found that the personal information at issue includes highly sensitive personal information which, if disclosed, could result in significant personal distress to the affected parties. With this in mind, I do not have sufficient evidence to conclude that the public interest in disclosure clearly outweighs the purpose of the section 14(1) exemption, which is to protect the privacy of individuals with respect to their own information held by government institutions.

[93] Accordingly, I find that there is no compelling public interest in disclosure that would outweigh the purpose of the personal privacy exemption under section 14(1).

ORDER:

I uphold the police's decision and dismiss the appeal.

Original Signed by: April 2, 2025

Anda Wang
Adjudicator