ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2006-033

October 13, 2010

EDMONTON POLICE SERVICE

Case File Number 3341

Office URL: www.oipc.ab.ca

Summary: An individual, a lawyer, brought a complaint that this name had been used by various members of the Edmonton Police Service (EPS) to run queries on police information systems, on nine occasions, in the absence of the authorization required by section 39 of the *Freedom of Information and Protection of Privacy Act*. He also complained that the security arrangements for personal information in relation to such queries were not in accordance with the requirements of section 38 of the Act.

The Commissioner reviewed the evidence in relation to the individual queries. He found that the EPS had demonstrated that it had authority under section 39 for conducting some of the queries, but that it had failed to demonstrate that it had authority for some of them, and that some of them had clearly been conducted for improper purposes and without authority. For one of these queries, the Commissioner also found that he did not believe the testimony of the member who had conducted the query.

With respect to reasonable security arrangements, the Commissioner held that the systems that were in place at the time the unauthorized queries were conducted were inadequate by reference to the requirements of section 38 both in terms of the training members had received as to the purposes for which running queries (and the associated collection and use of personal information) was permissible, and as to the absence of a requirement to give reasons and to enter the reason on the computerized information system.

With respect to the current position, the Commissioner found that EPS has developed security arrangements against unauthorized access to the system, and the associated unauthorized use of personal information, that generally meet the standards of section 38 of the Act.

The Commissioner declined to accept the Complainant's proposal that he impose a condition on the EPS that queries can be conducted only on the basis that the querant has a "reasonable suspicion", before running the query, that the information collected will advance a police or law enforcement purpose. In the Commissioner's view, this test was not preferable to the existing test for authority contained in the Act, nor was it necessarily appropriate for the kinds of queries that are commonly conducted.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss.33, 38, 39, 39(1)(a), 39(4), 41, 69(6), 72, 72(4), 92.

Orders and Decisions Cited: AB: Orders F2006-029, F2006-031, P2006-008, F2008-029; Decision F2010-D-001.

Court Cases Cited: *Bow Development Ltd. v. William Kelly and Sons Plumbing Contractors Ltd*., [2005] A.J. No. 1265; *Kellogg Brown and Root v. Alberta (Information and Privacy Commissioner)* [2007] A.J. No. 896; *Alberta Teachers' Association v. Alberta (Information and Privacy Commissioner)* 2010 ABCA 26.

I. BACKGROUND

[para 1] This inquiry arises in consequence of information provided to the Complainant by the Edmonton Police Service (the EPS or the Public Body) that his name had been run through the CPIC and PROBE information systems by various members of EPS, on 10 occasions, between 1999 and 2005. (Only nine queries are presently in issue, as the Complainant has not taken issue with one query conducted by a particular EPS member.) The Complainant says that the remaining nine queries were done without the authorization required by section 39 of the *Freedom of Information and Protection of Privacy Act*, ("the Act"), and that the EPS did not make reasonable security arrangements against such risks as unauthorized use, as required by section 38 of the Act.

[para 2] A notice of inquiry was issued in January, 2006, and the oral inquiry commenced on April 4, 2006. In the initial stages of the inquiry, the EPS conceded, in its written and oral submissions, that the burden of proof was upon it to establish authority under section 39. It also conceded that for some of the queries (those conducted by particular named police officers), it had failed to discharge its burden of showing that they had been conducted for a proper purpose. It also conceded that the failure to demonstrate compliance with the Act "constitutes a breach of section 39 of the FOIP Act". With regard to most of these queries, the EPS indicated that the particular officers who had conducted them had no recollection of the query or queries they had conducted, and that there were no records that would establish the reasons that they were done. For

one of the queries, the EPS stated that the explanation of the officer whose mobile unit had been used for the query was that it must have been done by someone else who had used the unit without his knowledge. The EPS took the position that in light of its concessions on these factual and legal matters, it was unnecessary to call as witnesses the individual members of the EPS who had conducted the queries in question.

[para 3] The Complainant took the contrary position – that it was necessary to call these querants as witnesses, to enable me to decide the issues before me in this case, and to allow me to make an appropriate order.

[para 4] After receiving and considering arguments from the parties on this question, I acceded to the Complainant's request that the individual EPS members be called to provide testimony as to the queries conducted by them or, in one case, on a mobile unit assigned to an individual officer. My decision letter on this issue, dated August 11, 2006, is attached to this order as Appendix A. The oral inquiry in this case continued on a series of dates throughout 2007.

[para 5] On May 9, 2007, the EPS raised the issue that a reasonable apprehension of bias had arisen. This was based on a comment made by a spokesperson for this office to the media in relation to the present inquiry, which was reported in the Edmonton Sun on May 8, 2007. The statement, made was: "If police are found guilty, Work will likely tighten controls on officers' use of the information systems".

[para 6] In the oral part of the inquiry, on May 23, 2007, I gave my oral reasons for my decision not to recuse myself on account of the allegation of bias. These reasons are attached in Appendix B to this order.

[para 7] On March 7, 2008, the EPS raised the objection that I had lost jurisdiction due to alleged non-compliance with the timelines in section 69(6) of the FOIP Act. This objection was based on the decision in *Kellogg Brown and Root v. Alberta (Information and Privacy Commissioner)* [2007] A.J. No. 896. After receiving and considering arguments from the parties on this question, I decided (for the reasons set out in Order F2006-031) that I had not lost jurisdiction, and continued with the inquiry. The EPS brought an application for judicial review of this decision, but a consent order was signed by myself and both the parties which stated that the application would be adjourned *sine die*, with an agreement that the EPS would be entitled to file a fresh or amended Originating Notice seeking judicial review of Order F2006-031 after the order on the merits had been issued in this matter.

[para 8] The oral inquiry proceeded on additional dates in 2009, and concluded on November 27, 2009.

[para 9] On February 18, 2010 and February 23, 2010, the EPS objected to the my continuing with the inquiry in this matter, on the basis that the time lines set out in the Act had been exceeded, and that the inquiry must be terminated by reference to the test set out in the Court of Appeal's decision in *Alberta Teachers' Association v. Alberta (Information and Privacy Commissioner)* 2010 ABCA 26 (the ATA decision).

[para 10] I found (for the reasons set out in Decision F2010-D-001) that the ATA decision did not apply, as the requirements of section 69(6) of the Act had been met on the facts of this case. I found, in the alternative, that if the requirements of the provision had not been met, and the ATA decision was applicable, that the presumption of termination that would have arisen was overcome in this case.

[para 11] The EPS brought an application for judicial review of this decision, but on July 9, 2010, it obtained an order from the Court extending the time in which to file an application for judicial review of Decision F2010-D-001, and entitling it to file an amended Originating Notice seeking judicial review of that decision within 45 days of receiving my final decision relating to the merits of this inquiry.

II. ISSUES

[para 12] The issues, as set out in the Notice of Inquiry, are as follows:

Issue A: Did the Public Body have the authority under section 39 of the Act to use the Complainant's personal information?

Issue B: Did the Public Body protect the Complainant's personal information by making reasonable security arrangements against such risks as unauthorized use, as required by section 38 of the Act?

III. DISCUSSION OF ISSUES

Issue A: Did the Public Body have the authority under section 39 of the Act to use the Complainant's personal information?

[para 13] Under section 33 of the Act, a public body has the following authority to collect information:

> *33 No personal information may be collected by or for a public body unless*
>
> *(a) the collection of that information is expressly authorized by an enactment of Alberta or Canada,*
>
> *(b) that information is collected for the purposes of law enforcement, or*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body.*

[para 14] Under section 39(1)(a), a public body may use personal information for the purpose for which it was collected or compiled, or for a use consistent with that purpose. Section 41 clarifies that, for the purposes of section 39(1)(a), a use of personal information is consistent with the purpose for which the information was collected or compiled if the use:

> *a. has a reasonable and direct connection to that purpose, and*
>
> *b. is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.*

[para 15] Thus, section 39 is met where the personal information is used for the purposes of law enforcement, or is necessary for an operating activity or program of the public body. As well, by reference to section 39**(**4), a public body may use the personal information only to the extent necessary to carry out its purpose in a reasonable manner.

[para 16] The information of the Complainant that was collected and used by the EPS in conducting the queries - his name, as well as some other identifying information - was his personal information.

[para 17] I must consider whether the EPS has shown that its collection and use of the Complainant's personal information was for a law enforcement purpose (or for a purpose relating to and necessary for an operating program of the EPS). I must also consider whether the EPS needs to show, for each of the queries, whether the extent of its use was appropriate for these purposes, and if it does need to show this, whether it has succeeded in doing so.

[para 18] The information on these questions was given by the EPS through its written submissions as well as through the testimony of some of the members of the EPS who had conducted the individual queries. I will deal with each of the individual queries below.

Detective Glena

[para 19] The authorization for this member's query using the Complainant's personal information is no longer in issue. In the Complainant's concluding written submission, he states: "It appears from the evidence that this query related to a legitimate investigation". In addition, the query was conducted in August, 1999, before the FOIP Act came into force in relation to the EPS.

Constables MacKechnie and Watson, Ms. Graham

[para 20] The Complainant states in his concluding submission that the evidence revealed no motives for the queries run by these individuals.

[para 21] Constable Watson gave his testimony in this matter in March, 2007. He stated that on the date on which he ran the query using the Complainant's name (May 2, 2003) he was working at the desk at the Old Strathcona station. He could not recall the query nor locate any information that would indicate why it was done. I note that the Complainant's testimony indicated that he has attended at the Old Strathcona station on a number of occasions for purposes such as reporting vehicle damage.

[para 22] Constable Watson also testified that he had received an official warning for running an improper query several years prior, and that since that time he had made it his practice not to run queries for any purposes unrelated to his official duties.

[para 23] Constable MacKechnie was also working on the desk at the Old Strathcona station on the date he performed a query relative to the Complainant (on October 31, 1999). He entered the Complainant's full name and birth date, which indicates he received this information from some source other than the database. He could not recall the reason for the query, nor find any information which would indicate why it had been done. Although the FOIP Act had only recently come into force, the Constable stated that he understood that the EPS policy at that time was that querying was for policing business only, not for personal matters.

[para 24] Ms. Graham conducted a query using the Complainant's name on January 20, 2003, while performing her duties as a clerk in the Police Information Check Unit. These duties were to process the names of individuals who are listed on EPS forms that are submitted for police information checks, which are generally done at the request of a third party, with their consent. She did not recall performing the query, and records of such checks were not maintained by EPS at the time. She testified that she did not know who the Complainant was, and would not have queried his name for any purpose other than the performance of her duties.

[para 25] Earlier orders of this office have held that even though an EPS member does not remember performing an individual query, where they give evidence that it is their practice to perform queries only in relation to their police work, and where there is no credible suggestion that there may have been an improper motive, a finding may be made that there was authority for the query in accordance with the requirements of section 39 of the Act. See, for example, Order F2006-029 and F2008-024.

[para 26] Based on the evidence set out above, I am prepared to accept that even though these individuals discussed above did not remember performing the queries, they conducted them for police purposes.

[para 27] However, it is my responsibility under the legislation to determine not only whether the purpose was a law enforcement purpose, but also whether the information was collected and used only to the extent necessary to carry out the law enforcement purpose in a reasonable manner, in accordance with the requirements of section 39(4).

[para 28] Thus, for example, if in a given case accessing the database information has only a very tenuous connection with the goal of law enforcement such as would not, on balance, justify the violation of privacy associated with the access of the information by the EPS member, using the information to carry out the purpose might not be carrying it out in a reasonable manner, and would not meet the terms of the provision.

[para 29] By way of example, it may be the case that the EPS routinely runs CPIC checks for all persons who are stopped by the police for traffic violations, and that this occasionally yields an outstanding warrant. The practice of running all such checks could be described as having a police purpose. However, if, hypothetically, only one warrant were encountered for every thousand or even every hundred checks, this practice arguably would not meet the test of using personal information only to the extent necessary for the EPS to carry out its law enforcement purposes in a reasonable manner.

[para 30] However, I am at present not in a position to effectively analyse this or any other of the myriad of possible policies and practices of the EPS relative to running database queries, in terms of their compliance with the "reasonableness" test in the Act. Doing so would require far more data as to why queries are being done in particular circumstances, and how the information that is accessed achieves police objectives. In the given example, I would need to know, for example, not only how often a query uncovers an outstanding warrant, but how pervasive outstanding warrants are, whether there are other mechanisms available for locating the subjects of warrants, whether and why it is important to do so in all or in some cases, and so on.

[para 31] These are questions which I could consider, at most, on a case-by-case basis, and even so, it would make sense to ask the question only in circumstances in which a complainant could initially show that for their particular circumstance, there is clearly a reason to question the access of the information in their case. In Order P2006-008, I said

> … it will be up to a complainant to adduce some evidence that personal information has been collected, used or disclosed. A complainant must also adduce some evidence about the manner in which the collection, use or disclosure has been or is occurring, in order to raise the issue of whether the collection, use or disclosure is in compliance with the Act.

[para 32] I adopt these statements for the present case. I will ask whether information has been used only to the extent necessary to enable enforcing the law in a reasonable manner only in circumstances in which the facts presented by the complainant fairly raise the "reasonable manner" issue. Proof that a query was done, if it was done for law enforcement purposes, will not in itself raise this issue. This conclusion is consistent with earlier orders of this office respecting police database searches, in which, for queries that were shown to have been done for law enforcement purposes, the adjudicators did not go on to require the EPS to demonstrate that the use of the information met section 39(4), as there was nothing raised by the complainants to suggest the query may not have been reasonably necessary to meet the law enforcement objective.

[para 33] Furthermore, it would be unfair to rule on the reasonableness for achieving policing goals of a particular database-searching incident or practice without giving the EPS an opportunity to present evidence and argument in support of what was being done.

[para 34] In addition, any such analysis would have to take into account that police need to be given space to make both policy and case-by-case decisions about when they need to access information in the database. This is so given the need to rely on intuition and experience, the need to react decisively and quickly in high-pressure situations, and the need to access as much information as possible that is relevant to safety concerns of the members themselves and of the public.

[para 35] Finally, I can see that there may be some merit in having standardized policies about the situations for which queries are to be done for law enforcement, so as to eliminate the need for officers to concern themselves about the possible repercussions of taking this step, as well as the need to balance, for every circumstance, whether a legal test has been met in the given circumstances of the case. Such careful weighing may not be practicable given the number of situations that arise in which this judgment would have to be made, and often made quickly.

[para 36] It does not follow from this observation that every such policy would be defensible, but it does follow that it might be acceptable, within the terms of the test, to apply generally-defensible policies routinely even though not every individual circumstance to which the policy applies would necessarily, of itself, meet the test. Thus, to take a hypothetical example (as I have no evidence on this point), the police may have a policy that queries are done routinely when a 911 complaint is made. This might be justifiable for many cases, as the information in the query may bear significantly on the assessment of a caller's credibility, or of other relevant factors that a 911 dispatcher is to consider. There may be individual circumstances in which such a check is clearly not merited, as might be revealed with the benefit of hindsight, but given the emergency-like nature of the calls, it may be acceptable to have a routine practice rather than requiring the 911 dispatcher to make a judgment as to whether to run the query for every case.

[para 37] On the basis of the foregoing, I find that the EPS has discharged its onus of showing that the collection and use of the information by Constables MacKechnie and Watson, and by Ms. Graham, was authorized within the terms of the Act.

Staff Sergeant Horne, Constable Mitchler, Sergeant Dick, Sergeant Boehnke

[para 38] I turn next to the evidence relating to a number of queries in which there is a dispute as to whether the query had a police purpose. For most of these queries, the EPS puts forward a police purpose, but the Complainant disputes that the purpose given by the EPS is the one that motivated the search, and, in each of these cases, he suggests an alternate purpose – one based on personal animus – which the Act does not authorize. I will review each of these queries.

1. Staff Sergeant Horne

[para 39] This member ran queries relative to the Complainant on March 27, 2000, while he was working as an investigator in the Internal Affairs Unit. In its initial submission, the EPS stated, based on its own internal investigation into these queries, that just prior to running it, Staff Sergeant Horne had received four complaints written by the Complainant, three of them relative to the same constable, and a fourth relative to two other constables. The EPS stated that the Staff Sergeant had conducted the queries because it was unusual to receive complaints authored by lawyers rather than by citizens, and because it raised questions as to who was the true complainant – the lawyer, or his clients. EPS argued that the Staff Sergeant was trying to determine whether there was a further connection between the Complainant and the constables about which he was complaining, and whether there was something driving the complaints other than the matters expressed in the letters of complaint, so as to assess the Complainant's credibility.

[para 40] The evidence also disclosed that the Complainant had lodged a complaint against Staff Sergeant Horne about the way in which he had investigated the complaints just discussed, but this latter complaint was not lodged until considerably after the Staff Sergeant had conducted the queries at issue (on April 17, 2000) .

[para 41] Evidence given by the Staff Sergeant during the oral part of the inquiry revealed that the complaints had come forward in the form of letters from the Complainant, and that the last two of these, though dated before the date of the queries, had in fact not been received by the Staff Sergeant and assigned to him for investigation until the day after he had run the queries. However, the Staff Sergeant testified that he believed it probable that he had been aware of the latter complaints at a date earlier than the queries, because they had arrived via fax, and possibly they would have become a topic of general discussion, before they were formally provided to him and signed off by him as the investigator for this series of complaints. He maintained this position despite the fact that counsel for the Complainant argued, based on the fax numbers on the documents, that the latter complaints had in fact been faxed to the Chief of Police rather than to the Internal Affairs unit in which the Staff Sergeant was working.

[para 42] As well, the evidence showed that on March 27, Staff Sergeant Horne met with a client of the Complainant, and obtained a 'complaint withdrawal form' from him, and that the Staff Sergeant also advised that client that his complaint could be addressed whether or not he had a lawyer, and suggested that the client should check whether the Complainant was billing the client for his services. As well, another staff sergeant provided evidence that it would be unusual to run a query relative to the lawyer of someone who had brought a complaint to the police.

[para 43] I acknowledge that the possibility that the latter two of the complaints were received only after the query was conducted would weaken to some degree the EPS's argument that the motive for the query was to discern who the "true complainant" was.

As well, I accept that the Staff Sergeant's suggestion made to the client that the Complainant may have been billing the client unnecessarily possibly carries the suggestion that the Staff Sergeant disapproved of the Complainant's involvement in the complaint process.

[para 44] Despite these points, however, I cannot conclude, based on the evidence before me, even on a balance of probabilities, that it is more likely than not that the Staff Sergeant's query was done other than for the police purpose of attaining more information about the complaints, in furtherance of the internal affairs investigation. The evidence as to when the Staff Sergeant became aware of the latter two complaints is inconclusive – possibly it was before he ran the queries. With respect to the point about unnecessary billing, even if this reflected disapproval of the Complainant's role, it does not follow that the Staff Sergeant was not truly trying to ascertain the nature of the complaints and the Complainant's motive in having made them. I find, on a balance of probabilities, that Staff Sergeant Horne conducted the query of March 27, 2000 for a policing purpose, and that the query was done only to the extent necessary to carry out the purpose in a reasonable manner..

2. Sergeant Dick

[para 45] The EPS stated in its initial submission that in its internal investigation in relation to this query, the Sergeant stated that he had no recollection of the query, and could find no evidence which would suggest the motivation behind it

[para 46] This member queried the Complainant's name on February 12, 2004, and shortly thereafter he scanned several violation tickets (primarily photo radar tickets) relating to the Complainant, using his date of birth obtained through the name query.

[para 47] The evidence established that at the time of the query Sergeant Dick was the supervising sergeant for a constable against whom the Complainant was pursuing allegations of misconduct. The constable's father - the then-acting police chief - was also concerned in the allegations insofar as the investigation into the son's conduct was done internally while he was acting Chief (which was the subject of an independent complaint brought by a client of the Complainant's associate).

[para 48] The Sergeant testified that he was aware of the allegations but had no direct involvement in the investigation, and was unaware of the dates of the related court proceedings or the status of the criminal matters. He said he did not discuss these with the constable other than possibly relative to the time the constable needed to take off for court.

[para 49] The Complainant suggests that the Sergeant's purpose in looking at the closed traffic violation files was to find out whether the Complainant had any outstanding warrants for unpaid traffic fines. Presumably the idea is that the search was motivated by animosity to the Complainant based on his role in the complaint against the squad member.

[para 50] I accept that there may be some question as to why the Sergeant would review the Complainant's closed traffic ticket files. No law enforcement purpose for such a review was suggested by the EPS. As well, there is no positive evidence from the Sergeant as to whether it was his invariable practice to conduct queries only for law enforcement purposes. Indeed, in Exhibit C in this inquiry, which is a chart summarizing the results of the search done in response to the Complainant's information request, there is an entry relative to Sergeant Dick that states that in a conversation with EPS counsel, he acknowledged doing inappropriate queries in the past, and that the query could have been in relation to the case involving the constable in his squad. (I do not know, however, who authored this document).

[para 51] In view of the foregoing evidence, I find that the EPS has failed to establish that the query in question was authorized.

[para 52] However, I do not believe there is enough evidence in this case to support the conclusion that the query was done for the purpose suggested by the Complainant. I agree, though, that if such a review were done simply because the Complainant was involved in a complaint against a squad member, this would be an improperly-motivated query. Even if it could be said of such a query that it was done for a law enforcement purpose in the sense that outstanding warrants could possibly have been located, this would not, under the circumstances, meet the Act's requirement that law enforcement purposes be carried out in a reasonable manner.

3. Constables Mitchler and Schriever

[para 53] Queries using the Complainant's name were conducted on November 11, 2003 (at 3:00 a.m. during a night shift) from a mobile unit that was at the time assigned to Constables Mitchler and Schriever. Constable Mitchler's notebook revealed that Constable Mitchler had recorded the Complainant's name, birth date, and address in his notebook during the shift in which the queries were done. Constable Mitchler indicated that he did not recall the queries, that at that time he had no specific knowledge of who the Complainant was, and that he had no reason to believe the queries were for an inappropriate purpose.

[para 54] Subsequently, the evidence revealed that on November 10, 2003, the day prior to that on which the queries were done, a trial was in progress in which the Complainant was acting as defence counsel and in which Constable Schriever had been involved as an investigator, and relative to which he was present in court (although he did not testify). The Constable testified that he had had some discussions with the prosecutor concerning that trial, possibly (though this point is not entirely clear) on the same day, and also stated that he would have become aware of who the defence counsel was on the day of the trial.

[para 55] After the conclusion of this trial, the Complainant made a complaint against Constable Schriever concerning the Constable's conduct in the investigation, and the Constable was ultimately given an official warning relative to this matter. The

Complainant now argues that the fact this trial was taking place on the day before the queries were done suggests that Constable Schriever had an improper motive for performing them. With respect to Constable Mitchler, presumably the Complainant's idea is that because Constable Mitchler wrote the Complainant's name and address in his notebook, he was also involved in the searches, for the same purpose.

[para 56] Neither Constable had entries in their notebooks with respect to any investigations they conducted during the shift in question. As well, Constable Mitchler did not provide evidence that it was his invariable practice not to conduct queries for other than police purposes. In fact, he indicated the contrary, when he explained that at the time the queries were done, checking someone's name was not "that big of a deal" as long as the information that was accessed was not disclosed to anyone else. He also set out some reasons why he had done checks, including on his own name, for purposes that he did not regard as police purposes. As well, the Constable testified that he had been given an official warning in relation to an unrelated matter (which took place later, in 2004) for having conducted an inappropriate query.

[para 57] Constable Schriever testified that he had no memory of searching the Complainant's name. He stated that if the search at issue had been in relation to a vehicle stop, a licence plate search would have been done, as it is routinely the practice to do licence plate searches for all vehicle stops. (Such a license plate search was in fact not done.) As was the case with Constable Mitchler, Constable Schriever gave no evidence that it was his invariable practice to conduct queries only for police purposes.

[para 58] In my view, the foregoing evidence is some evidence of a possible motive for Constables Mitchler and Schriever's having conducted the queries relative to the Complainant – that is, that they were done because Constable Schriever already had knowledge of the Complainant's concerns regarding his conduct in the investigation relative to the trial described above. I note as well that Constable Shriever's evidence is to the effect that the queries were not done in consequence of a vehicle stop. Also, the Complainaint has testified that he is certain that he did not have contact with the police at 3:00 a.m. on the night in question.

[para 59] If the available evidence permitted me to conclude that Constable Schriever actually knew about the impending complaint against him, or at least the Complainant's concerns that underlay it, at the time of the searches, I would be prepared to find, on a balance of probabilities, that this was the motivation for them (which would be an improper motive and would make the searches unauthorized). However, in the absence of such evidence, I do not feel I have enough on which to base a firm finding about the Constables' motivation.

[para 60] However, in view of the fact that Constable Mitchler could not assert that it was his invariable practice to conduct queries only for police purposes, and that Constable Schriever did not make any such assertion, I have no basis on which to find that the queries were done for an authorized purpose.

4. Sergeant (now Staff Sergeant) Boehnke

[para 61] Staff Sergeant Boehnke conducted a name query relative to the Complainant on March 29, 2000. The EPS indicated in its original submission that in the internal investigation related to this query, the Staff Sergeant stated that he had no specific recollection of performing it, and that he had no knowledge of the Complainant at the time. He also said that he had reviewed his files, as well as trials in which he had been involved, from the relevant time period and had found nothing that could assist him in determining the cause for the query.

[para 62] On March 7, 2007, Staff Sergeant Boehnke testified that, despite his best efforts, he had no recollection in respect of the query of the Complainant's name that he had conducted on March 29, 2000.

[para 63] Staff Sergeant Boehnke's query was among those concerning which the Complainant requested that the EPS perform "bracket searches". That is, for certain of the queries, the Complainant asked, during the course of the inquiry, that it be determined whether and what searches were done both immediately (15 minutes) before, and immediately after, certain of the searches already at issue in this inquiry. The EPS complied with this request. With respect to Staff Sergeant Boehnke's search, it was revealed that in close proximity to Sergeant Boehnke's search using the Complainant's name, he also searched variations of a phonetic spelling for a person named Lisa P… [Ms. P].

[para 64] In November, 2009, the Complainant forwarded an affidavit to the EPS, sworn by Ms. P, who is a lawyer. In this affidavit, Ms. P stated that she had been observing a trial in March, 2000, in which Staff Sergeant Boehnke had been a Crown witness. She said that in the course of this trial, Staff Sergeant Boehnke had had difficulty identifying one of the accused, and that she later overheard him talking about this to other officers outside the courtroom. It appears that Ms. P conveyed this information to the Complainant in his role as defence counsel. When Staff Sergeant Boehnke was recalled, he was asked whether he had had any conversations about misidentifying the accused outside the courtroom (which apparently would have involved a violation of the court's order excluding witnesses) and he denied doing so. The trial against the accused did not proceed, as the Crown ultimately withdrew the charges.

[para 65] Based on the results of these "bracket searches", as well as the affidavit of Ms. P relating thereto, Sergeant Boehnke was recalled to give further testimony on November 25, 2009.

[para 66] Upon being recalled, Sergeant Boehnke was reminded by counsel for the EPS of his previous evidence regarding his query. After reviewing further evidence, namely the "bracket searches", Ms. P's affidavit, and a partial transcript of the March 23, 2000 trial (at which he had been a witness, the Complainant had been counsel, and Ms. P had been a spectator and potential witness), Staff Sergeant Boehnke testified that while he

takes responsibility for the queries in question and does not deny making them, he still has no recollection of doing so and he cannot recall or explain their circumstances.

[para 67] In cross-examination, Staff Sergeant Boehnke reiterated the efforts he had made to refresh his memory at the time of the complaint in 2005, and agreed that he now knows of other approaches he could have taken to try to establish the cause. However, he maintained that he still has no independent, specific recollection of the trial or of the specific events referred to in Ms. P's affidavit, or of his reaction to or state of mind during those events.

[para 68] However, he indicated that he does not recall being accused of violating a court order at any other time in his career as a police officer. He also stated that, at the date of that trial, he knew both the Complainant's and Ms. P's names. Although he could not recall any other intervening events, Staff Sergeant Boehnke conceded that it was probable, and was "certainly possible", that the trial was the impetus for the queries in question (although he stated he would not exclude other possibilities).

[para 69] I find, on a balance of probabilities, on the basis of the foregoing evidence, and particularly Staff Sergeant Boehnke's concession regarding this probability, that the motive for his database query using the Complainant's and Ms. Ps names, in close proximity, was related to the courtroom incident described above. I am aware of no police purpose for such a query in the circumstances described, and none was suggested to me. Accordingly, I find that it was done for an unauthorized purpose rather than one authorized under section 39 of the Act, and as well, that it was done for a personal and improper motive.

5. Constable Zielie

[para 70] Queries relative to the Complainant were done from the mobile workstation in the vehicle then assigned to Constable Zielie on July 31, 2004, at 10:08, and again (as revealed by the "bracket searches" requested by the Complainant) at 10:15. (The second search was a scan of a case file that was in relation to a different matter relative to which the Complainant had brought a complaint to the EPS.)

[para 71] Constable Zielie denied having done these searches, and stated that they must have been done by someone else, during a period in which he says he left his car unlocked and the computer logged on and thus accessible to be used by someone else.

[para 72] According to the time as recorded on the "unit history", Constable Zielie logged off the computer at 10:15:35. According to the mobile workstation record of the time, the second of the searches was done at 10:15. It appears from these timing records that Constable Zielie is the only person who could have done the second search, and, since the first search was also in relation to the Complainant, that he also conducted the first search, contrary to his claim that he had not done either of them.

[para 73] The Complainant argues that Constable Zielie's denials are false. He says that the Constable had a clear motive for running the query using his name, which is that at the time of the query he was facing upcoming disciplinary hearings under the *Police Act* which had been initiated by the Complainant (which in fact took place in September, 2004). He says the timing of the second search (which closely coincided with the time at which Constable Zielie testified that he logged off the computer) puts beyond doubt that Constable Zielie conducted the queries

[para 74] Counsel for Constable Zielie argued that it had not been absolutely established that the second query was done in the same minute as Constable Zielie logged off the system. He provided evidence that CPIC searches as recorded on the workstation are timed on eastern time, and there is a two hour and two minute difference between the timing of a CPIC search as recorded in eastern time and the timing of a PROBE search as recorded in local time. As well, the unit history uses a different clock, and there is no way to establish the correctness of the clocks or the relationship between these various times. (This argument was in line with the findings in a disciplinary proceeding against Constable Zielie relative to giving false testimony in this inquiry. In that proceeding, the Presiding Officer found that the time of the searches could not be conclusively established, and therefore the possibility that the search was done by someone other than Constable Zielie could not be precluded. At the time the EPS made its final submissions, this finding was under appeal to the Law Enforcement Review Board.)

[para 75] Counsel for Constable Zielie also argued that this initial testimony should not be taken as testimony of his actual recollection of the events, but of his recollection after refreshing his memory from the unit history, and that there is some question as to whether Constable Zielie's testimony was that he logged of the system himself, or that he was saying only that the unit history showed that someone logged off at that time.

[para 76] As well, counsel for Constable Zielie argued that I do not have jurisdiction to recommend that Constable Zielie be prosecuted, and that there is insufficient evidence for me to make a finding which would support such a prosecution.

[para 77] Counsel for the Complainant replied that I should assume the times are accurate unless it is established otherwise. As well, he points to the fact that Constable Zielie had testified that he had logged out, and that the idea that this was not testimony as to his recollection should be discounted as having been contrived after the testimony had been given.

[para 78] In light of the evidence and arguments reviewed above, I find that Constable Zielie performed the searches in question. I make this finding taking into account that there may be some minor difference between the time the second search was done and the time at which, according to Constable Zielie's testimony, he logged off the computer.

[para 79] The primary consideration, in my view, is the presence of a motivation to look up the Complainant's information for an improper purpose. I have noted that Constable Zielie testified that at the time of the searches, he was unaware of any specific steps that

had been taken in the complaints relative to him that coincided with the date of the queries, and the EPS initially argued that since the complaints (as well as a civil action against him in which the Complainant was acting as counsel for the plaintiff) were initiated in 2000, the likelihood was low that animus motivated the search (performed four years later). However, it is notable in my view that at the time of the query a hearing of the Law Enforcement Review Board was due to be held (which was held in fact in September of 2004) at which a complaint against Constable Zielie (in which the Complainant was involved) was determined.[1] As well, at the time of the query, another complaint made by the Complainant to the Chief of Police was still outstanding.

[para 80] As well, I find it highly doubtful that a police officer would leave his police car unlocked, with the computer logged on, and equally doubtful that some other person, totally unknown to the Constable, would enter the car and use the computer to run a query relative to the Complainant. That this would be done by a non-EPS member seems completely out of the question. The idea that one constable would surreptitiously use the computer of another constable rather than using one he was himself entitled to access equally strains credulity, particularly in the absence of any requirement at the time that reasons be recorded. The only credible explanation is that Constable Zielie conducted the queries.

[para 81] I find, therefore, that these searches were done for an improper motive and hence were done without authority.

Conclusion regarding authority under section 39

[para 82] In accordance with the review of the evidence above, I find that the EPS has demonstrated that it had authority under section 39 for conducting some of the queries, but that it has failed to demonstrate that it had authority for some of them, and that some of them were clearly conducted for improper purposes and without authority.

Remedies sought by the Complainant

[para 83] The Complainant has asked that I recommend to the Minister of Justice and Attorney General that he conduct as investigation of possible offences under section 92 of the Act, and an investigation of possible criminal offences of perjury and obstruction of justice in relation to these proceedings, specifically in relation to the testimony of Constable Zielie and Staff Sergeant Boehnke.

[para 84] As explained above, I have found the testimony of Constable Zielie to be not credible. I believe that he conducted the queries discussed above and that he was untruthful about this in giving evidence before me in this inquiry. Though I have no duty to do so under the Act, and cannot be required to do so, it is possible for me (though not pursuant to any power granted to me under the Act) to swear an information to initiate an

[1] The resolution of this complaint was subsequently appealed and was unresolved as of the date of the Complainant's final testimony.

investigation or prosecution further to section 92 of the Act, or under the Criminal Code for perjury.

[para 85] However, the last date on which Constable Zielie gave testimony was in May, 2007. There is a two-year limitation period for commencing prosecutions under section 92, so the limitation period has elapsed. As for the Criminal Code, I note the evidence that consideration has already been given (in the form of a criminal investigation) as to whether the present situation was appropriate for a prosecution. However, I do not know what evidence and what other factors were taken into account in making that decision. While it is not part of the order in this case, it is my intention to inform the Crown of the facts relating to Constable Zielie's sworn testimony.

[para 86] I turn to Staff Sergeant Boehnke. The evidence shows that during a court proceeding in which he had been a witness, the Complainant raised issues about him which challenged his truthfulness and the lawfulness of his conduct in discussing his testimony outside the courtroom. Despite this, he testified that he did not recall these circumstances, nor did he recall having done the queries in issue at the time the matter was first raised with him in June, 2005. Indeed, he states that he still has no actual recollection of this.

[para 87] Given his testimony that this was the only instance in which a lawyer made such allegations relative to him, I have some difficulty believing that he did not remember the incident, and the related query, at the time he was first asked. Nonetheless, individual capacities for recollection differ, and I concede there is a possibility that his memory of this faded and was eventually obliterated by subsequent events. Thus while I have some reservations about accepting that Sergeant Boehnke was truthful in the testimony about his recollection of these events he gave before me (especially on the point that he still did not recall the circumstances or the related query even after being reminded about them), in the absence of any additional evidence, I can reach no firm conclusion about it. On this account, any action on my part respecting prosecution would be inappropriate.

Issue B: Did the Public Body protect the Complainant's personal information by making reasonable security arrangements against such risks as unauthorized use, as required by section 38 of the Act?

[para 88] Under this heading I will consider first whether at the time of the queries here at issue, the EPS had reasonable security arrangements in place with respect to safeguarding personal information against authorized use. I will also consider the current status. As well, I will address whether in making my order as to reasonable security arrangements, I ought to direct the EPS to adopt the "reasonable suspicion" test proposed by the Complainant before it may run a name query on a police database.

Security arrangements at the time the unauthorized queries were conducted

[para 89] The EPS has demonstrated that at the time of the queries in issue, it had taken some steps to ensure the appropriate use of personal information of the Complainant and others in his position. It argues that in view of the fact that at the time in question, the requirements of the FOIP Act were still quite new, and that the potential concerns regarding improper use by police officers were not yet known, the measures that had been taken at the time of the queries were reasonable, and in accordance with the requirements of section 38.

[para 90] However, this case has placed into high relief the inadequacies in the system that existed at the time the queries were done, both in terms of the understanding of the EPS members as to the appropriate limitations on use of the names of individuals to run police database queries, as well as in terms of the failure of the system in not requiring the reasons for queries to be recorded.

[para 91] Some of the queries were, as I have found, conducted for reasons of personal animus and thus for improper purposes. This indicates that at the time, it had not been fully brought home to the membership of the EPS that queries were to be limited to those relating to their official duties.

[para 92] As well, the absence of any requirement to indicate reasons or any ability to do so on the computerized information system has made it impossible for the EPS to conclusively demonstrate an authorized purpose for a large proportion of the queries that have been questioned, both in this case and in relation to other persons. While this office has thus far allowed some leeway by permitting testimony of members as to their general but invariable practices to substitute for demonstrated reasons, what has been revealed in this case makes it clear that the absence of reasons was a severe shortcoming that required a remedy.

[para 93] Thus, despite EPS's arguments to the effect that the newness of the legislation and the lack of appreciation as to the risk of inappropriate use of personal information were mitigating factors, I find that that at the time, the security arrangements against authorized access fell short to some degree of the "reasonableness" standard.

Current arrangements

[para 94] The EPS dedicated a considerable proportion of its efforts in this inquiry to demonstrating that the security arrangements it has made in relation to police information systems has significantly evolved. Accordingly, as it has raised this issue, I will comment on whether I believe these arrangements are adequate in terms of its duty under section 38 of the Act to protect personal information by making reasonable security arrangements against risks of unauthorized access, collection, use and disclosure. The detailed information the EPS provided as to what it has done or is continuing to do to ensure its future ability to meet the requirements of the Act is set out, in the form in which it was

provided to me in the EPS's concluding submission, dated November 26, 2009, in paras 118 to 146, in Appendix C to this order.

[para 95] In an earlier order (F2008-024) I asked the EPS to put proper systems in place to ensure that reasons for a query using an individual's name are entered into the system so there is no doubt about why the search was conducted. I expressed my view that reasons for a search must be clearly stated to enable the EPS to meet its obligations under the FOIP Act.

[para 96] Included in its closing submission, and appended thereto, is a service directive entitled "Completion of Reason for Access/Use in EPROS and EPROS Gateway". This directive states that the reason for access (which is a mandatory field) must be filled out in a manner that includes the factual, occurrence-specific reason for access (i.e. occurrence numbers and/or any comments as to why the query is being made). This meets the requirement that reasons be stated with sufficient particularity that it can be determined if the query was called for police purposes.

[para 97] I note as well, as is explained by the EPS more fully in the excerpt from its submission quoted in Exhibit C, that a random audit system has been put in place, and that disciplinary measures have been taken in cases where the rules have been transgressed which indicate to members that such breaches will not be tolerated. As well, in my view this proceeding, and others in which the authority for running queries has been challenged, have likely served to drive this point home to the membership of the police force.

[para 98] To conclude, security measures against unauthorized access have now been developed to a point that I believe meets the terms of section 38.

[para 99] This is not to say, however, that it is no longer possible for individuals to question whether any particular query met the terms of section 38 and 39. An individual who believes that their name was used to run a query that was not for an authorized purpose or was not reasonable for a police purpose, as discussed earlier at paras 31 and 32 may still bring a complaint to this office. As well, they may challenge whether the security arrangements were sufficient to guard against unauthorized use for a query of that particular type.

The proposed "reasonable suspicion" test

[para 100] Before concluding this part, I will address the suggestion of the Complainant that in view of what has been revealed through this inquiry about police practices relative to database searches, I ought to adopt the test for individual queries that the querant must have a "reasonable suspicion", before running the query, that the information collected will advance a police or law enforcement purpose.

[para 101] The Complainant asks that I place the following condition on the EPS:

> That the Edmonton Police Service immediately implement a policy whereby access to personal information by police officers must be limited to circumstances where the police officer has a reasonable suspicion that access to the information will advance a legitimate police purpose.

[para 102] The Act already contains a test for collection and use of personal information by public bodies.

[para 103] First, section 33 of the Act states that information may be collected for a law enforcement purpose. (In the present context, the "collection" is of the identifying information that is used to run a query.) This is an objective test, which requires that there be a law enforcement purpose; on a review of the collection by this office, the public body has the onus to demonstrate this purpose.

[para 104] With regard to use, section 39(1)(a) permits information to be used for the purposes for which it was collected or compiled. Assuming the information was collected for a law enforcement purpose, it may be used for this same purpose.

[para 105] Most importantly in the present context, section 39(4) requires that the use be only to the extent necessary to carry out the purpose in a reasonable manner. I take "to the extent necessary" in the present context to meant "insofar as it is necessary", rather than referring to degrees of use (which in the context of database searches would be meaningless). "Necessary" in the present context has been interpreted in earlier orders of this office as broader than "indispensable", and as satisfied where use of the information provides a means of achieving a law enforcement objective that would not otherwise be available.[2]

[para 106] For the reasons described below, I decline to adopt the test proposed by the Complainant.

[para 107] The test requires the querant to have a reasonable suspicion that running the query will advance a law enforcement objective before they may collect and use the identifying information to run the query. The test in the Act requires that running the query be necessary to enable the EPS to carry out law enforcement in a reasonable manner.

[para 108] The source of the "reasonable suspicion" test is cases in which the police have some reason to believe that if they conduct a search, they will find whatever it is they suspect is to be found – in other words, if it is found, it will confirm their suspicion.

---

[2] In Order F2008-029, the Adjudicator held that : "… I find that "necessary" does not mean "indispensable" - in other words it does not mean that the CPS could not possibly perform its duties without disclosing the information. Rather, it is sufficient to meet the test that the disclosure permits the CPS a means by which they may achieve their objectives of preserving the peace and enforcing the law that would be unavailable without it."

For example, it will reveal that an individual is implicated in the criminal activity that is under investigation. Possibly, what the Complainant means is that the police should not run queries unless they have a reasonable suspicion that the information that will be disclosed by the query will confirm some suspicion/theory they have about the involvement of the subject of the query in some particular matter to be true.

[para 109] However, many of the purposes described in the evidence of the EPS as to why searches are conducted for law enforcement purposes would not fit within this scenario, as they are not being done to confirm a suspicion. For example, possibly the police run queries to determine whether a person who has been stopped for a traffic violation has an outstanding warrant. Such queries would be precluded by the "reasonable suspicion" test because it would not be sensible to say that police "suspect" all people they stop for traffic violations of having outstanding warrants. Similarly, one would not "suspect" that any individual 911 caller is a crank or habitual caller, but one might run a query to ensure that they are not. In such situations, the police purpose for running the query can be articulated, but no "suspicion" is involved. Although not all such other purposes necessarily meet the "reasonable manner" element in section 39(4), as I have discussed above, I would need a great deal more evidence about the reasons for conducting the various kinds of queries the EPS describes before I would be prepared to reject them on the basis that they fall outside the limitation in section 39(4).

[para 110] If, alternatively, the Complainant means to propose a test that requires a "reasonable suspicion" that whatever is disclosed by running the query will give the police information that is useful for them to know for law enforcement purposes, I note that this would create a test less stringent than the one expressed in the Act – which requires that there be a law enforcement purpose in fact rather than merely a suspicion of one. Practically speaking, the situations in which these two tests are met might often coincide, but the "suspicion" test nonetheless theoretically covers a broader range of circumstances. I note in passing that the EPS made reference to the definition of "reasonable suspicion" in *Words and Phrases*[3], and that the definition quoted states the following:

> … something more than a "mere suspicion" and something less than "reasonable and probable grounds." It requires a subjective and objective assessment. It is equivalent to "articulable cause" and must be based on a constellation of objectively discernable facts. A "hunch" based on intuition gained by experience will not suffice.

[para 111] If this is a correct interpretation of the phrase "reasonable suspicion", then the "articulable cause" policy which is apparently already in place for running EPS queries would be equivalent to the "reasonable suspicion" test in any event. (However, I note again that a "suspicion" would not necessarily have arisen in all situations in which the law enforcement purpose for running a query could be articulated, and that the proposed test is therefore also too restrictive in its requirement that something be *suspected* before the query can be done.)

[3] Carswell, 2009.

[para 112] I note finally that the proposed test would not allow policies for routinely running queries in specified circumstances to be put in place. Again, I have no evidence as to whether and how this is done, but I have already noted some possible advantages of having such policies. The appropriate test for instituting a policy as to when to run queries routinely would be whether the policy is a reasonable one given the need to balance policing goals with individuals' privacy; again, "suspicion" is a concept that does not fit in the context, as suspicion would not necessarily have arisen in every situation in which the policy was to be applied.

[para 113] In reaching these conclusions, I have noted the argument of the EPS that the standard should be different when the information that is being accessed by the query is already in the hands of the EPS, and is simply being looked at by an individual member, rather than when police are searching for something they do not yet possess. The EPS appears to make this point in support of its argument against the "reasonable suspicion" test. I am rejecting this test in any event, but note that the point made by the EPS is unsupportable for two reasons.

[para 114] The first is that the information, the collection and use of which is being complained about in the present case, is the identifying information of the Complainant, rather than any information about him that exists in the database and was accessed by the search. For most of the queries there is no indication at all about what information may have been accessed and to what use it may have been put.

[para 115] The second reason is that the FOIP Act has provisions governing both use and collection of information, and it is the compliance with these provisions that is at issue in this inquiry. Even if the complaint were also about the use of information that existed in the database, the same principle would apply – the question would be whether the use was for a law enforcement purpose, and whether it had been done only to the extent necessary to carry out the purpose in a reasonable manner. The fact the information has already been collected does not detract from the obligation to meet these requirements for the use of personal information.

[para 116] To conclude, in my view, the introduction of the concept of "reasonable suspicion" does not add anything useful to the existing standards articulated in the Act, and also has the potential to import confusion. Indeed, I regard it as inconsistent with those standards, in the ways I have described. I will therefore not apply it, nor will I suggest that the EPS should implement it.

Other remedies requested by the Complainant

[para 117] The Complainant requested two additional remedies:

- that I require the EPS to implement a requirement that police officers must record who is accessing personal information, and their reason for doing so at the time of or immediately following the access, and;

- that I require the EPS to immediately implement proper recording, control and spot auditing programs to ensure access is limited to circumstances that meet the "reasonable suspicion" test proposed by the Complainant.

[para 118] In my view the first requirement has already been met by the EPS in that Service Directive "Completion of Reason for Access/Use in EPROS and EPROS Gateway" specifies that the reason for access must be specified when logging onto the system and/or when initiating a new search or query, subject to certain limited exceptions for EPROS Gateway.[4] As well, querants must identify themselves using their regimental or payroll numbers.

[para 119] With respect to spot audits, the EPS has told me it has implemented a random audit process, which is overseen by the Executive Director of the Office of Strategy Management, a newly created position within the EPS, and has communicated to its members that such a program exists via a Service Directive ["Compliance Check of Information Systems"]. I have dealt with the "reasonable suspicion" aspect of this part of the Complainant's request earlier.

IV. ORDER

[para 120] I make this Order under section 72 of the Act.

[para 121] I find that the EPS has shown that it had authority within the terms of section 39 of the Act with regard to the queries conducted by Ms. Graham, Constables Watson and MacKechnie, and Staff Sergeant Horne.

[para 122] I find that the EPS failed to show that it had authority within the terms of section 39 of the Act with regard to the queries conducted by Sergeant Dick, and Constables Mitchler and Shriever. I find that Staff Sergeant Boehnke and Constable Zielie conducted queries for improper purposes, and hence that these queries were not authorized within the terms of section 39.

[para 123] I find that the systems that were in place at the time the unauthorized queries were conducted were inadequate by reference to section 38 both in terms of the training members had received as to the purposes for which running queries (and the associated collection and use of personal information) was permissible, and as to the absence of a requirement to give reasons and to enter the reason on the computerized information system.

[4] The exceptions are where a member must process large numbers of queries (in which case an exception must be approved) or where the reason is recorded instead in their notebook or electronic device that is accessible for audit purposes.

[para 124] I find that the EPS has since developed security arrangements against unauthorized access to the system, and the associated unauthorized use of personal information, that generally meet the standards of section 38 of the Act. However, this office will continue to consider, if asked, whether the standard was met in individual cases in which there is a challenge as to a particular use of information.

Frank Work, Q.C.
Information and Privacy Commissioner

Appendix A: Decision letter regarding the requirement that querants give evidence at the inquiry

August 11, 2006

Mr. Simon Renouf, Q.C.
Simon Renouf Professional Corporation
300, 10020 – 101A Ave.
Edmonton, Alberta T5J 3G2

Ms. Katrina Haymond
Field LLP
200, 10235 – 101 Street
Edmonton, Alberta T5J 3G1

Dear Mr. Renouf and Ms. Haymond:

Re: Review Number 3341 - Preliminary Issue: Should the Commissioner require the police officers who have not yet appeared before him, whose names appear in the chart of queries provided to the Complainant by the Public Body, to attend and provide evidence in this Inquiry?

1. Background:

This Inquiry arises in consequence of information provided to the Complainant by the Edmonton Police Service (the "Public Body") that his name had been run through the CPIC and PROBE information systems by various members of the Edmonton Police Service, on a number of occasions, between 1999 and 2004. The Complainant says that these queries were done without the authorization required by section 39 of the *Freedom of Information and Protection of Privacy Act* ("the Act"), and that the Public Body did not make reasonable security arrangements against such risks as unauthorized use as required by section 38 of the Act.[5]

An inquiry was commenced and in that inquiry, the Public Body conceded, in its written and oral submissions, that the burden of proof was upon it to establish authority under sections 38 and 39. It also conceded that for some of the queries (those conducted by particular named police officers), it had failed to discharge its burden of showing that they had been conducted for an authorized purpose. It also conceded that the failure to demonstrate compliance with the Act "constitutes a breach of section 39 of the FOIP Act". With regard to most of these queries, the Public Body indicated that the particular

[5] Section 38 requires a public body to make reasonable security arrangements against unauthorized use of personal information. Section 39 specifies the limited circumstances under which a public body may use personal information.

officers who had conducted them had no recollection of the query or queries they had conducted, and that there were no records that would establish the reasons that they were done. For one of the queries, the Public Body stated that the explanation of the officer whose mobile unit had been used for the query was that it must have been done by someone else who had used the unit without his knowledge. The Public Body takes the position that in light of its concessions on these factual and legal matters, it is unnecessary to call as witnesses the individual members of the EPS who conducted the queries in question.

The Complainant takes the contrary position that it is necessary to call these officers as witnesses, to enable me to decide the issues before me in this case, and to allow me to make an appropriate order.

2. Discussion of the Issue

As the basis for its concession that it could not meet its burden of proof, and therefore that it had breached section 39 of the FOIP Act, the Public Body conceded the following facts:

- At the time the queries were conducted, the EPS information systems did not allow the user to enter a reason for the query directly into the system.
- The EPS audit logs do not indicate a reason for the query.
- The EPS can only determine the reason for the query if the person conducting the query recalls performing the query, or if there is independent evidence (such as a note in a notebook) that provides some assistance.
- The EPS has not called any evidence that would establish the precise reason for the queries.

As well, the EPS stated in its submissions that when questioned, in most of the cases, the individual officers stated that they did not recall the reason for the query they had conducted.[6]

In my view, the Public Body's concessions about factual matters do not correspond with its legal conclusions. Neither do they permit me to make a conclusive determination of the issues before me, of whether the Public Body had authority under section 39 of the Act to use the Complainant's personal information in the queries it conducted, and whether it made reasonable security arrangements against unauthorized use.

I note first that it is not a breach of the Act to fail to meet a burden of proof. Rather, it is a breach of the Act to use information for an unauthorized purpose. The Public Body has not conceded that, through its employees, it had used information for an unauthorized purpose. At most it says that it cannot establish conclusively whether the purposes were authorized or not. The failure to prove that something is true does not as a matter of logic prove its converse. I do not see, therefore, how the concession by the Public Body that it cannot prove the purposes were authorized leads to a conclusion that the individual queries that were run were unauthorized and thus involved a breach of the Act.

[6] In one case, the officer stated that he had not conducted the query run through his mobile unit, and that this must have been done by someone else.

I note as well that at the same time as the Public Body concedes it has not met its burden, it makes suggestions about the particular searches that they likely were for an authorized purpose. First, for some of them, it notes that the birth date of the Complainant was used as a search term (which, it says, was probably obtained through contact with the Complainant, or from his driver's licence). Second, for some of them, it says that the search term was the Complainant's first and last name only, which (because this name may be common with that of other people) does not establish that the Complainant was the person whose name was searched. Both these suggestions are meant to disprove the idea that the searches were for an unauthorized purpose. They suggest the purpose was, or was likely, proper but simply cannot be remembered. Thus, the Public Body is not conceding the information was used for an improper purpose. Therefore, again, the concession does not, in itself, allow me to make a finding on the question before me – of whether the information was used for a purpose that was or was not authorized (and whether the Act was or was not breached). The Public Body itself asserts, at paragraph 20 of its Reply Brief, that "Pursuant to Part 5, the Commissioner must determine whether the [Public Body] used the Complainant's personal information for a purpose that is not authorized by the FOIP Act". My duty is to make this finding on the basis of all the available, relevant, evidence.

Another problem with the Public Body's contention relates to my ability to exercise my powers under section 72(4), which permits me to "specify any terms or conditions" in an order. I take this provision as allowing me to impose requirements relative to the Public Body's information management practices as these relate to its ability to meet the terms of the Act. In this case, any evidence that might provide information as to the nature of deficiencies in these practices could be relevant to the terms and conditions I choose to impose. Thus, it would be relevant to know whether the particular queries at issue involved willful use contrary to the Act, improper usage resulting from ignorance of the Act's requirements, or, as the Public Body seems to suggest, were likely proper uses that could not be shown to be such because they were not adequately documented. Any suggestions as to changes of practice would be informed by which of these scenarios describes the queries at issue.[7] The testimony of individual witnesses who ran the queries may well throw further light on this question. Indeed it may do so even if I accept that they do not recall the particular incidents.

I note as well that my jurisdiction involves the "resolution" of complaints. This aspect of my powers is meant, in part, to ensure the Complainant's concerns about the use of his information are satisfactorily addressed. In my view, a preliminary step for a satisfactory resolution is to try to discover how the information was used. This is certainly so from the standpoint of the Complainant – part of his concern is not knowing how his information was used. The Public Body says that I need not go beyond its factual concession that, in its own investigation of the matter, it could not find out what the

[7] It is arguable that I should only point out any inadequacies in information management and leave it to the Public Body to decide how to remedy them, but even if this is what would be best, I still need to know where the shortfall lies. The evidence of the individuals is clearly relevant to this question.

purposes of the queries were. Conceivably, the officers' direct answers on these points, or answers to the complainant's cross-examination, could shed more light on these questions than has already been illuminated by the Public Body's concessions.

I turn finally to the Public Body's point that it is beyond my jurisdiction and my experience to deal with the conduct of individuals (as opposed to the conduct of the Public Body), and with willful violations of the Act. In this regard, I make the following observations.

First, the Public Body acts through its individual employees. If an individual employee breaches the Act in the course of his or her employment, the Public Body breaches the Act. My role in this proceeding includes examining the Public Body's information management practices and the extent to which these are effective to prevent breaches of the Act by its employees. However, that is only one of my roles. My jurisdiction is to answer all questions of fact and law arising during the course of the inquiry. Thus I must try to determine if the Act was breached and how it was breached. In a situation such as this one, this can be done only by examining what the individual employees of the Public Body did. Much of the evidence presented by the Public Body pertains to this very question. However, it suggests that because it has determined through its own investigation that it is impossible to establish the answer conclusively, I may not go beyond this assertion to discover for myself what the individual employees did. I am not willing to abdicate my role as a finder of fact about this key point to the Public Body.

With respect to the idea that it is not within my jurisdiction to act as a substitute disciplinary body for improper conduct of individual police officers, I agree with this point. However, in this case, examining conduct which could at the same time become the subject of a disciplinary proceeding is simply an incidental result of the proper exercise of my jurisdiction. The fact that there is another forum for dealing with police disciplinary matters does not curtail my ability to deal thoroughly with matters that are properly before me. It is not within my jurisdiction to ensure that improper conduct of police officers is disciplined, but it is within my jurisdiction to ensure that the Public Body, through its employees, deals with information properly and in accordance with the Act. If, during the course of an inquiry, willful inappropriate conduct is revealed, there is a process in place to deal with that. It is not improper for me to consider the related information unless I do it solely for the purpose of disciplining officers. That is not my purpose here.

A failure to consider relevant evidence can be an error of law and breach of natural justice which results in a loss of jurisdiction. It cannot be said, before hearing the evidence of individual witnesses as to what happened in the individual queries, that they have no evidence to give either on direct examination or cross-examination, beyond that conveyed by the Public Body in its submissions, that is relevant to the factual and ultimately the legal questions I must decide. In view of this, I reject the Public Body's contention that I should not call these witnesses because to do so would not be a judicious use of resources and would unnecessarily prolong the proceedings.

3. Preliminary Ruling

Accordingly, I will comply with the Complainant's request that I require the officers whose names appear on the chart of queries, and who have not yet appeared before me, to attend and to provide evidence as to the queries conducted by them or, in one case, on a mobile unit assigned to an individual officer. The evidence of these witnesses is relevant to the issues of which notice has already been given, and there is no need at this point to expand the scope of the Inquiry.

Yours truly,

Frank Work, Q.C.
Information and Privacy Commissioner

Appendix B: Decision on reasonable apprehension of bias

The Edmonton Police Service raised the issue of reasonable apprehension of bias on May 9, 2009, based on a comment by the office spokesperson that appeared in the Edmonton Sun on May 8, 2007. The statement was that: "If police are found guilty, Work will likely tighten controls on officers' use of the information systems".

In the oral part of the inquiry, on May 23, 2007, I gave my oral reasons for my decision not to recuse myself.

My decision was based on the law in Alberta as expressed by the Alberta Court of Appeal decision in *Bow Development Ltd. v. William Kelly and Sons Plumbing Contractors Ltd*., [2005 A.J.] No. 1265 at para 5. The Court articulated the test as follows: "if a reasonable person, properly informed, viewing the matter realistically and practically, and having thought the matter through, would think it more likely than not that the decision maker, whether consciously or unconsciously, would not decide fairly" there is a reasonable apprehension of bias.

Applying this test, in my view, the conditionals "if" and "likely" that are contained in the impugned statement detract from any certainty as to what my ruling will be, and thus the statement would not likely give rise to apprehension that I will not decide fairly.

Furthermore, I am entitled to look at this from point of view of reasonable person *properly informed.* In my view, a properly informed person would be aware that from the outset, the EPS stated that things have been tightened up (since the queries at issue were performed), and that there was a need to tighten things up, in particular to articulate a law enforcement purpose prior to a search. This point of view, which the EPS held in the first place, is demonstrated in policy (see Tab 29, Exhibit A [EPS Initial Submission dated March 20, 2006], and reiterated, among other places, in para 124 of Exhibit A (which refers to EPS Policy and Procedure Part 5).

As a properly informed person would regard what was said as a foregone conclusion given EPS submissions in the first place, such a person would not think it likely that I would not decide fairly.

Frank Work, Q.C.
Information and Privacy Commissioner

Appendix C: Excerpt from the closing submissions of the EPS regarding security arrangements against unauthorized access to the information system
Case File #F3341

118. At the time the queries were conducted, the EPS' internal information system was PROBE. In June of 2006, PROBE was replaced by EPROS. Therefore, security arrangements that are presently in place, and that were in place at the time of the queries, are addressed below.

119. The security arrangements in place at the EPS can be grouped into several different categories: log-in procedures and timeouts, EPS policies and procedures, training initiatives, spot audits, and disciplinary proceedings.

(i) Log-in Procedures

120. At the time the queries were conducted, access to both PROBE and CPIC was restricted by individual log-in identification procedures. PROBE log-in protocols required two unique identification features: the user's payroll number and password. Passwords had to be changed every six months. There is a similar log-in procedure for the EPROS system.

121. Inspector Ratcliff also provided evidence concerning the warning that appears when members first long [sic] onto EPROS. Each time a user logs into the system, a warning comes up advising that the use must be for a police related purpose […]. Both PROBE and EPROS also automatically time out if it takes a user too long to enter his or her log-in information.

122. Both PROBE and EPROS also automatically time out if it takes a user too long to enter his or her log-in information.

123. The log-in procedures and the automatic time-out feature reduce the possibility that an unauthorized person could access the system.

(ii) Policies and Procedures

124. In addition, the EPS has administrative safeguards in place against unauthorized use in the form of EPS Policy and Procedure and Service Directives.

125. Service Directives are bulletins distributed to each EPS member electronically on the EPS network via e-mail. Hard copies of the Service Directives are maintained in accessible locations (e.g. notice boards or binders) in each division […]. Service Directives may contain policy change information or simply items of interest, information or direction […].

126. EPS Policy 15-A-3 requires all EPS members to read and comply with Service Directives […].

127. In 2002, the policy in place with respect to security of Information […] stated the following:

> The security of our information systems (including those external systems to which we subscribe) is the responsibility of all members. All access, input, inquiry and use must be police related.

128. As of 2002, there was no requirement that members be able to articulate the police-related purpose any time a police information system was used.

129. In January of 2004, that policy was amended and the following was added: "Members must be able to clearly articulate the police-related purpose any time an information system is used." […].

130. The EPS has continued to modify and expand its policies with respect to accessing police information systems, partially in response to concerns raised by members of the public that police information systems were being accessed for inappropriate purposes.

131. Three policies were introduced in March of 2006 addressing these issues:

- The first was EPS Policy and Procedure 5-S-19 Mobile Workstations (MWS). That policy specifically requires that EPS members ensure that police vehicles are locked when left unattended; that the MWS "lock" feature is activated; and that they take all necessary precautions required to ensure unauthorized persons do not view information displayed on the MWS screen […].

- In addition, EPS Policy and Procedure 11-A-4 Conflict of Interest provides guidance to EPS members about conducting queries on EPS information systems in situations where the member may be in a conflict of interest […].

- In addition, EPS Policy and Procedure Part 5-Introduction, 3. Security of Information and Policy 5-C-1 Introduction to CPIC was intended to provide specific guidelines to members regarding the appropriate and inappropriate reasons for conducting a query […]. The policy was issued to all members by way of a Service Directive. The Policy provides specific examples of queries that are both appropriate, and inappropriate.

- The Policy also specifically establishes that members must be able to articulate the law enforcement purpose any time an information system is used. While this was also a requirement in the 2004 policy […] it was very difficult for members to meet this requirement, given that the PROBE system did not have a field where a member could enter a reason for conducting a particular query. The EPROS system (which became operations in June of 2006) included a "reasons" field to assist members in tracking the reasons for the their [sic] queries. Accordingly, while this requirement was in place as of 2004, the EPS did not have the technology to assist members in fulfilling this requirement until more recently.

132. In addition to the above, the EPS issued a further Service Directive concerning Compliance Checks of Information Systems on June 26, 2006 […]**.** The Service Directive indicates that random checks will be conducted to ensure that information systems are being used for law enforcement purposes.

133. In May of 2008, the EPS issued a further Service Directive concerning Completion of Reason for Access/Use in EPROS and EPROS Gateway […]. The Service Directive specifies that the reason for access must be specified when logging onto the system and/or when initiating a new search or query, subject to certain limited exceptions.

134. Each of the members who testified during the course of this Inquiry were asked whether they were now aware that queries could only be conducted in accordance with the Service Directive pertaining to Accessing Police Information, and whether the Service Directive provided sufficient clarity regarding the rules that apply to use of police information systems. All of the witnesses who testified indicated that the Service Directive was clear, and provided appropriate guidance. In addition, the members all indicated that they were using the "reasons" field to assist them in being to articulate the reason for a particular query, if asked about it subsequently. [emphasis in original]

135. These policies, and the introduction of a "reasons" field in EPROS, are important components of the "reasonable security" arrangements that are currently in place regarding use of police information systems.

136. While the members may have benefited from the earlier introduction of some of these policies, the EPS submits that concerns regarding the potential misuse of police information systems were not well known at the time the FOIPP Act came into force with respect to the EPS. Therefore, at the time most of the queries were conducted, the policies in place were reasonable.

137. Once concerns regarding the potential for inappropriate use of police information systems became better understood, the EPS took steps to introduce and communicate new policies to its membership regarding appropriate and inappropriate uses of information.

138. The delay in issuing the new policies was reasonable, given that the FOIPP Act was only introduced in 1999, and the EPS could not be expected to understand the implications of the new legislation immediately thereafter. The EPS' understanding of the legislation and its implications for law enforcement has matured and evolved over time, which has resulted in policies that are consistent with the requirements of the legislation.

139. The policies that were in place at the time queries were conducted were reasonable at that point in time, and the delay in introducing these policies does not prove that there was a breach of s. 38.

(iii) Training Initiatives

140. The EPS also has a number of training initiatives in relation to proper use of police information systems. Louise McCloskey, from the FOIPP Unit, provided *viva voce* evidence in regard to these initiatives, which can be summarized as follows:

- In 1998 and 1999, in anticipation of the EPS becoming subject to FOIP on October 1, 1999, all members of the EPS, both civilian and sworn, were provided with mandatory FOIP Awareness Training […]. Various sessions were provided based on the individual's role with the EPS. The various sessions provided were two hours, a half-day, a full day or two full days in duration. The first round of training consisted of general access and privacy training as the legislation was new to the EPS. It covered such things as access, privacy, collection, use, disposal, and corrections to personal information.

- Currently, the EPS FOIP Unit provides a two-hour training session on FOIP to all new EPS recruits with an emphasis on accessing various electronic systems.

- Victim Services Unit volunteer "Advocates" are provided with a two-hour information session as part of their yearly training curriculum. However, the EPS notes that most victim services advocates do not have access to CPIC or PROBE.

- Ongoing direction on the protection of personal information is provided to EPS members through various publications including:

    - Service Directives;

    - "Fast Facts" Bulletins: Fast Facts is a weekly bulletin produced by the EPS Public Affairs Unit and is distributed to all EPS members every Wednesday by e-mail. Fast Facts often contains information and directions to members regarding the security of personal information and the use of EPS information systems. See for example, the June 27, 2005, September 13, 2005 and January 4, 2006 issues of Facts Facts [sic] […];

    - "Severed Words": the EPS FOIP Unit's newsletter. The newsletter is designed to provide EPS members with up-to-date information about privacy issues and is distributed service-wide […].

- The EPS also maintains its own FOIPP Unit headed up by the EPS FOIPP Coordinator. There are currently four full-time staff members in the FOIPP Unit including the FOIPP Coordinator, two Disclosure Analysts and an Administrative Assistant. Staff from the EPS FOIPP Unit are available to consult with all EPS members regarding privacy and access issues at any time.

141. In addition, evidence was provided by Insp. John Ratcliff regarding a more recent training initiative that was provided to all members when EPROS became operational. Insp. Ratcliff testified that the EPS used EPROS training as a further opportunity to reinforce the rules relating to appropriate access to police information systems, as those rules are set out in the policies referred to above. The slides from the information that was provided to EPS members during the course of the EPROS training are at **Exhibit GG**. [emphasis in original]

(iv) Spot Audits

142. Sgt. McMechan provided evidence with respect to the spot audit project that was being considered when the Inquiry first commenced in March of 2006.

143. Since then, the EPS has implemented a random audit process, which is overseen by the Executive Director of the Office of Strategy Management, a newly created position within the EPS. Moreover, the EPS has communicated to its members, via Service Directive [“Compliance Check of Information Systems”] that such a program exists.

(v) Discipline

144. Another indication that there are reasonable security measures in place includes the fact that the Chief has made it clear that using police information for inappropriate purposes will not be tolerated.

145. In June of 2005, the Chief issued a special edition of Fast Facts in which he specifically stated that "anyone accessing information systems for purposes other than law enforcement, leaves themselves open for sanctions" […].

146. The Chief has disciplined those members who have been found to have violated the rules regarding appropriate access to police information systems. Attached is a decision of a Presiding Officer and a decision of the Law Enforcement Review Board which confirm that the Chief has disciplined members for inappropriate use of police information systems in appropriate circumstances [TAB 10: ‘*In the matter of a complaint and disciplinary proceedings against Regimental Number 1707 Constable Collin SMART’*].