Office of the Information and
Privacy Commissioner of Alberta

Investigation Report F2014-IR-01

Investigation into “Project Operation Warrant Execution” for compliance with the Freedom of Information and Protection of Privacy Act

March 17, 2014

Edmonton Police Service

Investigation F6148

Table of Contents

Introduction

[1] The Edmonton Police Service (EPS) launched Project Operation Warrant Execution (Project OWE) in March 2012. Project OWE was initially implemented in two stages.

[2] During Stage 1, which ran from March 5-31, 2012, individuals were encouraged to come forward and address their outstanding warrants.

[3] Stage 2 began on April 2, 2012. In this stage, the EPS publicly disclosed information identifying individuals with outstanding warrants. The media subsequently reported that the EPS had published information that identified a young offender and that the publication of the young offender's identity without a court order would constitute a violation of the *Youth Criminal Justice Act* (YCJA).

[4] The YCJA is a federal statute that prohibits the disclosure of information about young offenders who are involved in proceedings under the YCJA. Alberta's Information and Privacy Commissioner (the Commissioner) has no jurisdiction to investigate whether a disclosure of information is in contravention of the YCJA.

[5] The EPS, however, is a "public body" subject to the *Freedom of Information and Protection of Privacy Act* (the FOIP Act or Act). Under section 53(1)(a) of the FOIP Act, the Commissioner may "conduct investigations to ensure compliance with any provision of this Act."

[6] On April 4, 2012, the Commissioner issued a news release announcing she had decided to conduct an investigation on her own motion on the Project OWE initiative. The Commissioner said:

> The purpose of this investigation is to make sure this initiative is being carried out in compliance with FOIP, and that consideration has been given to the protection of personal information.

[7] The Commissioner also said:

> The investigation is not focused on the disclosure of information relating to particular individuals, however if people feel their personal information was released under this initiative in contravention of FOIP, they can make a complaint to my office and we will investigate.

[8] Our Office received no complaints from individuals about the disclosure of their information by the EPS under Project OWE.

[9] The Commissioner authorized me to investigate this matter. The objectives of the investigation were to:

- obtain an understanding of the purpose and intent of the Project OWE campaign;
- examine the management of personal information by the EPS and the measures taken to protect personal information against risks such as unauthorized access, collection, use and disclosure; and
- make recommendations, if necessary, to ensure that the EPS' management of personal information under Project OWE is in accordance with the provisions of the FOIP Act.

[10] My investigation found that the EPS did not make reasonable security arrangements to protect personal information as required under section 38 of the FOIP Act when it implemented Project OWE in 2012. My investigation also found that the EPS had authority to disclose some, but not all, of the personal information in Project OWE. I also found that the EPS did not limit the extent of personal information disclosed to what was necessary to carry out its purposes in a reasonable manner.

[11] Based on my findings, I recommend that the EPS:

- complete and submit a Privacy Impact Assessment (PIA) to our Office for review prior to undertaking Project OWE again or any new initiative involving the public disclosure of personal information;
- establish a policy for requiring PIAs when designing major projects or initiatives that involve the collection, use or disclosure of personal information prior to the implementation of the project; and
- develop a review and approval process that includes the EPS FOIPP Coordinator/FOIPP Office in initiatives or projects that involve the collection, use or disclosure of personal information.

Background

[12] The EPS first introduced warrant execution initiatives in the early 1980s.[1] In 2012, the EPS decided to implement Project OWE as part of its "Violence Reduction Strategy" to deal with the large volume of outstanding warrants in Edmonton and to specifically target the "top 100" (or so) highest offenders. [2]

[13] The EPS said it had more than 16,000 outstanding warrants in the Edmonton area ranging from failures to remove snow to more serious offences such as assaults, robbery, and firearms offences. The EPS determined Project OWE was the most efficient and effective means to address the large number of outstanding warrants.

[14] The EPS said the objectives of Project OWE were to:

- hold individuals accountable for their offences and specifically target those involving violence;
- inform those with outstanding warrants that the public's help would be enlisted by releasing their names and showing their photographs; and
- show the public that the police are removing the most dangerous offenders off the streets.

[15] During Stage 1 of Project OWE, which ran from March 5-31, 2012, the EPS published information on its website and through other media to encourage individuals to come forward and address their outstanding warrants by April 2, 2012, "or risk the possibility of having their names and faces advertised publicly and police visiting their home and workplace." [3] The EPS also stated, "people should deal with outstanding warrants by April 2, 2012. If people do not come forward to police of

[1] The FOIP Act was not enacted in the early 1980s, and therefore did not apply to the early operation warrant execution initiatives.
[2] The EPS established the "Violence Reduction Strategy" in response to the challenge of addressing violent crime in the City of Edmonton.
[3] Edmonton Police Service, copyright 2012, Warrants – Frequently Asked Questions, Retrieved on 04/04/2012. From http://www.edmontonpolice.ca/News/Warrants/FAQ.aspx

their free will, they will run the risk of public embarrassment. The EPS will be advertising the names of some people who have outstanding warrants in local newspapers."[4]

[16] On April 2, 2012, the EPS implemented Stage 2 and began publishing personal information of individuals with outstanding warrants in various local newspapers and on the EPS website. For example:

- on April 2, 2012 in the *Edmonton Sun*, the EPS published an advertisement with the names and ages of five individuals under the heading "DO YOU KNOW THESE PEOPLE?" Above each individual's name was either a photograph of the individual's face, or the word "SOLVED". The advertisement read, "These people have outstanding criminal warrants. If you have any information regarding the whereabouts of these individuals, or if one of them is YOU, contact your local police division or visit…"

- on the EPS website, the names, ages, photographs, heights and weights of several individuals were published under the following statement: "The following is a list of individuals who have yet to address their outstanding warrants. Stage 1 of Project OWE afforded individuals an opportunity to step forward and deal with their outstanding warrants. Stage 2, which commenced Monday, April 2, 2012, will see the Edmonton Police Service step up its enforcement efforts to locate these individuals, both in person and by advertising the photos and names in various publications and online."[5]

[17] On November 15, 2012, the *Edmonton Journal* reported that the EPS launched a subsequent stage of Project OWE which focused on individuals wanted for serious or violent offences and serious traffic infractions.[6] The EPS said no personal information was published for this stage of Project OWE.

[18] The EPS informed our office:

> The access and disclosure of the personal information for Project OWE was necessary and reasonable in order to address the approximately 16,000 outstanding warrants. The project was concluded and deemed to be an incredible success with more than 5,600 warrants being executed. Whether or not this project will be done again has not yet been decided.

Issues

1. Is the information at issue "personal Information" as defined in the FOIP Act?

[19] During various stages of Project OWE, the EPS disclosed some or all of the following personal information of up to 170 individuals: name, age, photograph, height, weight, and that the individual had an outstanding warrant.

---

[4] Edmonton Police Service, copyright 2012, Warrants – Frequently Asked Questions, Retrieved on 04/04/2012. From http://www.edmontonpolice.ca/News/Warrants/FAQ.aspx

[5] Edmonton Police Service, copyright 2012, Project: Operation Warrant Execution, *Reduced Crime and Victimization – Citizen-Centered Service – Model of Efficiency and Effectiveness,* Retrieved on 04/04/2012. From http://www.edmontonpolice.ca/CrimeFiles/ProjectOWE.aspx

[6] Pruden, Jana G. (Thursday, November 15, 2012). 'Blitz targets hundreds of wanted people in city'. Three arrests launch new phase of Operation Warrant Execution. *The Edmonton Journal,* pg. A5.

[20] The FOIP Act defines "personal information" as recorded information about an identifiable individual. "Personal information" under the FOIP Act includes an individual's name (section 1(n)(i)), age (section 1(n)(iii)), physical description (OIPC Order F2002-001, p. 10[7]), photograph (OIPC Order F2002-001, p. 10), and information about the individual's criminal history (section 1(n)(vii)).

[21] I find that the information disclosed by the EPS under Project OWE is "personal information" as defined in the FOIP Act.

2. Did the EPS comply with section 38 of the FOIP Act (reasonable security arrangements)?

[22] Section 38 of the FOIP Act states:

> 38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

[23] Unauthorized access to personal information includes:

- access by the public, where there is no right to access;
- access by a public body's employees, if those employees do not need to see the personal information in the course of their duties (OIPC Investigation Report F2003-IR-003, pp. 30-31);
- situations in which information is stored in an unsecured manner such that someone can obtain unauthorized access.[8]

[24] Unauthorized disclosure means disclosing personal information in ways other than those allowed under section 40 of the Act (OIPC Order 98-002, p. 198 and Investigation Report F2012-IR-01, p. 28).

Measures taken by the EPS to protect personal information

[25] The EPS described the process it undertook to select individuals for Project OWE. The following is a summary of this process:

- a download was received from the Canadian Police Information Centre (CPIC) Operations Alberta/NWT.
- the EPS CPIC Warrant Unit (CWU) sorted the records electronically to identify the current outstanding warrants. Once sorted electronically, a manual process was undertaken to select individuals for Project OWE. The CWU used the following criteria to identify the individuals for Project OWE: serious charges (assaults, robbery, firearms offences) with an Edmonton address in the Edmonton Police Records Occurrence System (EPROS).
- once the individuals were identified, warrants were copied and the CPIC Operators conducted a recent address check in EPROS as to determine the individual's whereabouts. An additional name check was then required through CPIC to ensure that the warrants were still outstanding.
- the CWU identified 170 individuals for Project OWE and forwarded warrant information packages for these individuals to the Project OWE team. The Project OWE team reviewed the packages and determined which individuals would be publicly identified.

---

[7] Orders and Investigation Reports mentioned in this investigation report are available on our office's website at www.oipc.ab.ca.
[8] See Orders 98-002, p. 136 and F2009-048, p. 92).

[26] As part of my investigation, the EPS provided me with copies of their policies and procedures that deal generally with the protection of personal information and compliance with the FOIP Act. These policies and procedures address (among other things): access controls; security of information, systems, networks, and buildings; CPIC information; disposal of information; destruction of reports; audits; access requests; FOIP requests; release of information; accountability and compliance requirements. In my view, the EPS' general policies and procedures support overall privacy management.

[27] From my review of these policies and procedures, however, I noted, and the EPS confirmed, that it does not have a specific policy that identifies when a privacy impact assessment (PIA) is required. A PIA process is a due diligence exercise in which a public body identifies and addresses potential privacy risks that may occur in the course of the project. A PIA is not mandatory under the FOIP Act, but our Office has consistently recommended that PIAs be completed for major projects that involve the collection, use or disclosure of personal information.[9]

[28] The Office of the Privacy Commissioner of Canada, and the Offices of the Information and Privacy Commissioners of Alberta and for British Columbia have published *Getting Accountability Right with a Privacy Management Program* to provide consistent guidance for private-sector organizations on the key components of a privacy management program. This guidance is also relevant for public bodies. The following excerpt is particularly relevant to the EPS:

> We have seen instances of organizations offering new services that collect, use or disclose personal information that have not been thoroughly vetted from a privacy perspective. Proper use of risk assessment tools can help prevent problems. Fixing a privacy problem after the fact can be costly so careful consideration of the purposes for a particular initiative, product or service, and an assessment that minimizes any privacy impacts beforehand is vital.
>
> As a result such assessments should be required throughout the organization for all new projects involving personal information and on any new collection, use or disclosure of personal information. Organizations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk assessments.
>
> Organizations should develop procedures for conducting such assessments, and develop a review and approval process that involves the Privacy Officer/Office when designing new initiatives, services or programs. For larger organizations, the Privacy Officer should be aware of the review process, and where there are high-risk initiatives, services or programs, the Privacy Office should be directly involved.[10]

[29] In reviewing the process undertaken to design and implement Project OWE, I find little or no assessment was made by the EPS as to their obligations to protect personal information as required under section 38 of the FOIP Act. I found nothing to demonstrate that prior to implementation there was an assessment of the legal authority and purposes for each element of personal information to be disclosed under the initiative. In addition, I found nothing to demonstrate consultation with, or involvement of, the EPS' FOIPP Coordinator/FOIPP Office prior to the implementation of Project OWE or the public disclosure of personal information.

---

[9] http://www.oipc.ab.ca/pages/PIAs/Description.aspx

[10] Office of the Privacy Commissioner of Canada and Offices of the Information and Privacy Commissioners of Alberta and British Columbia. *Getting Accountability Right with a Privacy Management Program.* April 2012. Page 12. Retrieved from http://www.oipc.ab.ca/Content_Files/Files/Publications/Accountability_Doc_April_2012.pdf

[30] Furthermore, the EPS also disclosed the name (first and surname) and age of individuals who no longer had outstanding warrants. Information about these individuals was publicly published under the word "Solved".

[31] I was informed by the EPS that the release of these individuals' names under the word "Solved" on April 2, 2012 was "not the preferred approach" and:

> The recommendation for any similar projects in the future will be to not release personal information of individuals unless there is an outstanding warrant or other law enforcement reason for the disclosure.

[32] The EPS' response reinforces my view that the EPS did not conduct an assessment of the legal authority and purposes for each element of personal information disclosed under Project OWE prior to the public disclosures.

[33] As a result, I find that the EPS did not fulfill its obligation under section 38 of the FOIP Act to make reasonable security arrangements to protect personal information when it implemented Project OWE.

3. Was the EPS authorized under the FOIP Act to disclose personal information as part of Project OWE?

[34] As noted above, during the two stages of Project OWE, the EPS disclosed all or some of the following personal information of up to 170 individuals: name, age, photograph, height, weight, and that the individual had an outstanding warrant.

[35] The EPS said it disclosed the personal information for the purpose of enlisting the public's assistance in addressing outstanding warrants.

[36] The EPS states the disclosure of personal information for Project OWE was authorized by the following provisions of the FOIP Act: 40(1)(b), 40(1)(c), 40(1)(e), 40(1)(k)(i) and 40(1)(ee). I reviewed the application of each of these provisions identified by the EPS.

Section 40(1)(b) (disclosure not an unreasonable invasion of personal privacy)

[37] Section 40(1)(b) states:

> 40(1) A public body may disclose personal information only…
>
> (b) if the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 17,

[38] Under section 40(1)(b), a public body may disclose personal information if the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 17 of the Act. In determining whether a disclosure of personal information would be an unreasonable invasion of a third party's privacy, a public body must consider sections 17(2), 17(4) and 17(5) of the FOIP Act.

Section 17(2) (disclosure not an unreasonable invasion of privacy)

[39] Section 17(2) of the Act lists the circumstances in which the disclosure of personal information is not an unreasonable invasion of a third party's privacy. I reviewed section 17(2) and find that none of the provisions under section 17(2) apply to the disclosure of personal information under Project OWE.

Section 17(4) (disclosure presumed to be an unreasonable invasion of privacy)

[40] Section 17(4) of the Act lists the circumstances in which the disclosure of personal information is presumed to be an unreasonable invasion of privacy. If the disclosure of personal information is presumed to be an unreasonable invasion of privacy, the public body must then consider and weigh all relevant circumstances as required under section 17(5) to determine whether a disclosure is an "unreasonable invasion of a third party's privacy".

[41] I find that sections 17(4)(b) and 17(4)(g)(i) are relevant. These sections read as follows:

> 17(4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if…
>
> (b) the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation…
>
> (g) the personal information consists of the third party's name when
>
> (i) it appears with other personal information about the third party…

[39] Under section 17(4)(b), a disclosure of personal information is presumed to be an unreasonable invasion of a third party's privacy if the personal information is an identifiable part of a law enforcement record, except if the disclosure is "necessary to dispose of the law enforcement matter or to continue an investigation."

[40] On this issue, the EPS stated:

> …the disclosure was not an unreasonable invasion of personal privacy. Warrants are judicial authorizations to arrest people to bring them before the criminal justice system. Individuals in these circumstances do not have a reasonable expectation of privacy in order to evade arrest. The FOIPP Act is not intended to aid fugitives from the justice system…

[41] In the case of Project OWE, the EPS disclosed that certain individuals had outstanding warrants; I agree with the EPS that this information is "an identifiable part of a law enforcement record" and that addressing outstanding warrants is part of "dispos[ing] of the law enforcement matter." However, under this provision, the disclosure must be "necessary". EPS provided no information to demonstrate that the disclosure was necessary. Therefore, the presumption of an unreasonable invasion of privacy does apply to disclosures of personal information for individuals with outstanding warrants.

[42] In addition, the presumption of an unreasonable invasion of privacy also applies to disclosures of personal information of those individuals who no longer had outstanding warrants.

Section 17(4)(g)(i) (disclosure of an individual's name in conjunction with other personal information)

[43] Section 17(4)(g)(i) of the FOIP Act states that a disclosure of personal information is presumed to be an unreasonable invasion of a third party's privacy if the disclosure consists of the individual's name when it appears with other personal information about the individual.

[44] As noted above, during the two stages of Project OWE, the EPS disclosed all or some of the following personal information of up to 170 individuals: name, age, photograph, height, weight, and that the individual had an outstanding warrant. I therefore find the disclosure of the personal information is presumed to be an unreasonable invasion of privacy pursuant to section 17(4)(g)(i).

Section 17(5) (requirement to consider all relevant circumstances)

[45] In Order F2007-028, former Commissioner Frank Work said:

> [para 15] When information falls under one of the provisions in section 17(4) of the Act, disclosure of the personal information is presumed to be an unreasonable invasion of a third party's personal privacy…However, as noted above, section 17(4) creates a presumption only. A Public Body must then consider the factors under section 17(5), as these factors may outweigh a presumption…

[46] Section 17(5) states:

> 17(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body <u>must consider all the relevant circumstances</u>, including whether
>
> (a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny,
>
> (b) the disclosure is likely to promote public health and safety or the protection of the environment,
>
> (c) the personal information is relevant to a fair determination of the applicant's rights,
>
> (d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,
>
> (e) the third party will be exposed unfairly to financial or other harm,
>
> (f) the personal information has been supplied in confidence,
>
> (g) the personal information is likely to be inaccurate or unreliable,
>
> (h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant, and
>
> (i) the personal information was originally provided by the applicant. [my emphasis]

[47] Section 17(5) sets out a non-exhaustive list of circumstances. Some of the circumstances weigh in favor of disclosure and some weigh against disclosure. Section 17(5) may rebut some of the presumptions that arise under section 17(4) of the Act.

[48] With respect to the relevant circumstances considered by the EPS in deciding to disclose personal information through Project OWE, the EPS said "[i]ndividuals in these circumstances do not have a reasonable expectation of privacy in order to evade arrest." In my opinion, this is a broad statement that provides no information as to what relevant circumstances the EPS considered as required under section 17(5).

[49] I find that the EPS could not rely on section 40(1)(b) since the EPS has not demonstrated how the disclosures would not be an unreasonable invasion of privacy.

Section 40(1)(c) (disclosure for the purpose for which information was collected or a consistent use)

[50] Section 40(1)(c) of the Act permits public bodies to disclose personal information for the purpose for which the information was collected or compiled or for a use consistent with that purpose. The section reads as follows:

> 40(1) A public body may disclose personal information only…
>
> (c) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,…

[51] The EPS said the disclosure is authorized by section 40(1)(c) because:

> …the information obtained through CPIC was collected for a law enforcement purpose. Using that information for the law enforcement purpose of executing warrants is consistent with that purpose.

[52] The EPS is saying section 40(1)(c) applies since the information was collected for law enforcement purposes and the disclosures through Project OWE were also for law enforcement purposes.

[53] I find that the disclosure of personal information in order to execute warrants is for the purpose for which the information was collected. As such, section 40(1)(c) authorized the disclosure of personal information of individuals with outstanding warrants. However, section 40(1)(c) did not authorize the disclosure of personal information of individuals who no longer had outstanding warrants.

Section 40(1)(e) (disclosure to comply with an enactment)

[54] Section 40(1)(e) of the Act allows a public body to disclose personal information for the purpose of complying with an enactment of Alberta or Canada.

> 40(1) A public body may disclose personal information only…
>
> (e) for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada,

[55] The EPS states the disclosures under Project OWE were for the purpose of complying with section 38 of the *Police Act.* Section 38 of the *Police Act* reads:

> 38(1) Every police officer is a peace officer and has the authority, responsibility and duty
>
> (a) to perform all duties that are necessary
>
> (i) to carry out the police officer's functions as a peace officer,

(ii) to encourage and assist the community in preventing crime,

(iii) to encourage and foster a co-operative relationship between the police service and the members of the community, and

(iv) to apprehend persons who may lawfully be taken into custody,

and

(b) to execute all warrants and perform all related duties and services.

(2) A police officer has jurisdiction throughout Alberta…

[56] I agree that section 38 of the *Police Act* places a duty on every police officer to execute warrants. However, I could not find a direct relationship between complying with the *Police Act* and disclosing the individual's information to the public. In other words, the disclosures cannot be said to be for the purpose of complying with the *Police Act,* because section 38 of the *Police Act* does not require the EPS to publicly disclose information through Project OWE.

[57] As such, I find that section 40(1)(e) did not authorize the EPS' disclosure of personal information through Project OWE.

Section 40(1)(k)(i) (disclosure to collect a fine or debt)

40(1) A public body may disclose personal information only…

(k) for the purpose of

(i) collecting a fine or debt owing by an individual to the Government of Alberta or to a public body, or to an assignee of either of them,

[58] Under section 40(1)(k)(i), a public body may disclose personal information for the purpose of collecting a fine or debt owing by an individual to the Government of Alberta or a public body, or to an assignee of either of them.

[59] The EPS said section 40(1)(k)(i) would permit the disclosure because, "some warrants have a fine associated to them and warrant execution results in collecting those fines".

[60] In my view, the disclosures for the purpose of collecting a fine may have merit for individuals with outstanding warrants. However, the EPS said "some warrants have fines associated to them"; in other words, not all individuals whose information was disclosed had fines or debts owing. The EPS did not confirm whether all individuals whose information was disclosed had fines or debts owing. Furthermore, section 40(1)(k)(i) would not authorize disclosures of personal information where the individuals no longer had outstanding warrants.

[61] I find that section 40(1)(k)(i) of the FOIP Act authorized the disclosure of personal information for those individuals with outstanding warrants that had fines associated with them.

Section 40(1)(ee) (disclosure to avert or minimize harm or imminent danger)

[62] At the time of the disclosures in 2012, section 40(1)(ee) read:

> 40(1) A public body may disclose personal information only…
>
> (ee) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person,

[63] For section 40(1)(ee) to authorize the disclosure of personal information, the following requirements must be met: the head of the public body must believe, on reasonable grounds, that there is an imminent danger to someone, and that the disclosure will avert or minimize that danger.

[64] In Order F2012-01, the Adjudicator said:

> [para 39] …in order for section 40(1)(ee) of the Act to apply in a given case, the head of a public body must believe, on reasonable grounds, that a danger or risk to the physical or psychological health or safety of others is present, or will be present in the relatively near future…"imminent" is a relative term…
>
> [para 40] Finally, for a public body to have the authority to disclose personal information under section 40(1)(ee) of the Act, its head must believe, on reasonable grounds, that the disclosure will "avert or minimize" an imminent danger to the health or safety of any person. In other words, the disclosure to the particular person or body must serve the purpose of averting or minimizing the imminent danger. There must be a link between disclosing the personal information and averting or minimizing the danger…

[65] Consequently, the EPS needed to demonstrate how the individuals whose information was disclosed presented an imminent danger to the health or safety of someone else and how the disclosure of these individuals' information would avert or minimize the danger. The general statement by the EPS that "violent offenders evading the justice system poses (sic) danger to the safety of the citizens of the City of Edmonton and Project OWE minimized some of those dangers" does not meet the requirement of section 40(1)(ee) of the Act.

[66] Furthermore, as noted earlier in this report, the *Edmonton Journal* reported on November 15, 2012 that the EPS launched a subsequent stage of Project OWE which focused on individuals wanted for serious or violent offences and serious traffic infractions. However, the EPS did not publicly release these individuals' personal information. If the EPS did not rely on section 40(1)(ee) to disclose the personal information of "individuals wanted for serious or violent offences and serious traffic infractions" then it is unclear how the EPS could rely on section 40(1)(ee) for the disclosures in April 2012.

[67] As such, I find section 40(1)(ee) did not authorize the disclosure of personal information for the purpose of Project OWE.

4. Did the EPS disclose personal information only to the extent necessary, in compliance with section 40 (4) of the FOIP Act?

> 40(4) A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in subsections (1), (2) and (3) in a reasonable manner.

[68] Section 40(4) requires that a public body disclose personal information only to the extent necessary to carry out an authorized purpose in a reasonable manner.

[69] I said earlier that, in my view, section 40(1)(c) of the FOIP Act authorized the EPS to disclose personal information about individuals with outstanding warrants and section 40(1)(k)(i) authorized the EPS to disclose personal information about individuals that had fines associated with their outstanding warrants. However, under section 40(4), the EPS must ensure it limits the disclosure of personal information to the extent necessary to carry out the purposes in a reasonable manner.

[70] In reviewing the various stages of Project OWE, I noted that the extent of personal information disclosed was inconsistent. For example, the personal information that appeared in newspaper advertisements included name, age and photograph. Information that was disclosed on the EPS website included name, age, photograph and also height and weight. No personal information was disclosed during the third stage of Project OWE that was launched in November 2012, and which targeted individuals wanted for serious or violent offences and serious traffic infractions.

[71] The EPS did not provide any explanation for why the disclosure of specific personal information elements was necessary. Furthermore, the inconsistency in personal information disclosures at various stages of Project OWE indicates that the EPS did not limit its disclosure of personal information to the extent necessary to enable it to carry out its purposes in a reasonable manner, thereby contravening section 40(4) of the Act.

Findings and Recommendations

[72] The findings from my investigation are as follows:

- the EPS did not fulfill its obligation under section 38 of the FOIP Act to make reasonable security arrangements to protect personal information when it implemented Project OWE.
- section 40(1)(c) authorized the EPS to disclose personal information for those individuals who had outstanding warrants.
- section 40(1)(k)(i) of the FOIP Act authorized the EPS to disclose personal information for those individuals with outstanding warrants that had fines associated with them.
- even though authorized to disclose some personal information of individuals with outstanding warrants, the EPS did not limit its disclosure of personal information to the extent necessary to enable it to carry out its purposes in a reasonable manner, thereby contravening section 40(4) of the Act.
- the EPS disclosed personal information in contravention of section 40(1) of the FOIP Act when it disclosed personal information of individuals who no longer had outstanding warrants.

[73] Based on my findings, I recommend that the EPS:

- complete and submit a PIA to our Office prior to undertaking Project OWE again or any new initiative involving the public disclosure of personal information. Among other things, the PIA should include the legal authority and purposes for each element of personal information to be disclosed for the project, and should identify the privacy risks and mitigation measures for the project. I suggest that the EPS refer to this office's publication, *Privacy Impact Assessment Requirements* as a guideline to write the PIA. [11]

[11] Office of the Information and Privacy Commissioner of Alberta. *Privacy Impact Assessment Requirements*. Retrieved from http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf

- establish a policy for requiring privacy impact assessments when designing major projects or initiatives that involve the collection, use or disclosure of personal information prior to the implementation of the project.
- develop a review and approval process that includes the EPS FOIPP Coordinator/FOIPP Office on initiatives or projects that involves the collection, use or disclosure of personal information.

[74] Upon the EPS' acceptance of these recommendations, I believe the risks to privacy for Project OWE and other similar projects and initiatives will be addressed.

Veronica Chodak
Senior Information and Privacy Manager