ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2020-30

October 14, 2020

ALBERTA JUSTICE AND SOLICITOR GENERAL

Case File Number 002687

Office URL: www.oipc.ab.ca

Summary: The Complainant, who appears as an agent in traffic court, complained that the Public Body had used his personal information in contravention of the FOIP Act when it diverted his request for disclosure in a traffic court matter on behalf of clients to its Corporate Security branch, and that it had disclosed his personal information in contravention of the FOIP Act when it included an email from the Corporate Security branch referring to the Complainant as a "complex client" in a disclosure package he had requested on behalf of clients.

The Adjudicator found that the Public Body had not collected or used the Complainant's personal information when it diverted his request for disclosure to the Corporate Security branch, as the request for disclosure was made by the Complainant acting in a representative, rather than a personal, capacity.

The Adjudicator found that the reference to the Complainant as a "complex client" was about the Complainant in a personal capacity and she found that including this information in a disclosure package intended for the Complainant's clients contravened Part 2 of the FOIP Act.

The Adjudicator ordered the Public Body to ensure that it did not include emails of this kind from Corporate Security in Crown disclosure packages in the future, absent authority under section 40 to do so.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 1, 38, 40, 72

Authorities Cited: AB: Order F2013-51

I. BACKGROUND

[para 1] The Complainant complained to the Commissioner that his personal information had been collected, used, and disclosed in contravention of Part 2 of the *Freedom of Information and Protection of Privacy Act*. He stated:

> On or around March 15th, 2016, [the Complainant] discovered that Corporate Security for the Crown ("Corporate Security") has been relaying or causing to be used, collected, disclosed, relayed and disseminated, communications and publications, referring to [the Complainant] as a "complex client" to third parties, including to the Calgary Crown Prosecution Office, who have been including such emails within the traffic ticket disclosure packages of clients for [the Complainant]. (Please see attached Exhibit "A") It should be noted that this is not the first time that the above has occurred.

The Complainant attached an email originating from Corporate Security and addressed to the Calgary Traffic Court division of Alberta Justice Crown Prosecution Services. This email refers to the Complainant as a "complex client" and explains that his request for disclosure on behalf of his client was referred to Corporate Security for "monitoring". The email explains that the disclosure request is legitimate and has been referred to the Traffic Court division for action.

[para 2] The Complainant also attached an email he sent to Corporate Security objecting to its use of the term "complex client" to describe him and also objecting to the fact that the email referring to him in these terms had been included in his client's disclosure package.

[para 3] The Commissioner authorized a senior information and privacy manager to investigate and attempt to settle the matter. At the conclusion of this process, the Complainant requested that the matter proceed to inquiry. The Commissioner agreed to conduct an inquiry and delegated her authority to conduct it to me.

II. ISSUES

Issue A: Did the Public Body collect the Complainant's personal information? If yes, did it do so in compliance with or in contravention of section 33 of the Act?

Issue B: Did the Public Body collect the Complainant's personal information directly or indirectly? If indirectly, did it do so in compliance with or in contravention of section 34 of the Act?

Issue C: Did the Public Body use the Complainant's personal information? If yes, did it do so in compliance with or in contravention of section 39 of the Act?

Issue D: Did the Public Body disclose the Complainant's personal information? If yes, did it do so in compliance with or in contravention of section 40 of the Act?

III. DISCUSSION OF ISSUES

Issue A: Did the Public Body collect the Complainant's personal information? If yes, did it do so in compliance with or in contravention of section 33 of the Act?

Issue B: Did the Public Body collect the Complainant's personal information directly or indirectly? If indirectly, did it do so in compliance with or in contravention of section 34 of the Act?

[para 4] In his complaint, the Complainant lists the collection of his personal information as an aspect of his complaint. However, he provided no description of the personal information he considered improperly collected.

[para 5] The Complainant's concern, as he set it out in his complaint, is that when he sends requests for disclosure to the Crown on behalf of the clients he represents in traffic Court, these requests are sent to the Public Body's Corporate Security branch, which scrutinizes the request. The Corporate Security Branch then determines whether the disclosure request may be acted upon by the Crown prosecution services branch. One such determination states:

> The attached Email is from [the Complainant] who is a known complex client to Corporate Security Services and his Emails have been re-directed for monitoring. There are times when [the Complainant's emails] are legitimate due to his current employment as a Traffic Ticket adviser and if the Email appears legitimate the Email will be forwarded for action. As indicated, the enclosed Email appears legitimate and is forwarded for your action.

According to the Complainant, the Public Body included this email in the Complainant's client's disclosure package. The Complainant's complaint is one regarding the scrutiny to which the disclosure requests are subjected by the Public Body's Corporate Security Services branch and the inclusion of information referring to him as a "complex client" in a Crown disclosure package. This is a complaint about *use* and disclosure of personal information within the terms of the FOIP Act.

[para 6] I understand that the Complainant anticipated that when he sent the requests for disclosure to the Public Body, the Public Body would collect his contact information for the purpose of providing disclosure. He did not anticipate that this information and the fact of his clients' involvement in a traffic matter would then be provided to the Public Body's corporate security branch for review before the disclosure package would be provided. It appears that the Complainant referred to "collection" in his complaint for the sake of completeness; the facts he outlines in his complaint do not

ground a complaint regarding the Public Body's collection of his personal information, but rather, its use and disclosure, As a result, I will not address the issues set out in the notice of inquiry regarding collection, but will address the complaint as it relates to the Public Body's use and disclosure of information about the Complainant.

Issue C: Did the Public Body use the Complainant's personal information? If yes, did it do so in compliance with or in contravention of section 39 of the Act?

[para 7] Section 39 of the FOIP Act sets out the circumstances in which a public body may use personal information. It states, in part:

> *39(1) A public body may use personal information only*
>
> *(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,*
>
> *(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or*
>
> *(c) for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43.*
>
> *[…]*
>
> *(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.*

[para 8] The Public Body argues:

> The CSRS [Corporate Security and Recovery Services] is authorized to use the Complainant's personal information in compliance with section 39(1)(a) and (4) of the FOIP Act which requires that a public body may use personal information for the purpose for which the information was collected or compiled or for a use consistent with that purpose. The CSRS used the Complainant's personal information only to the extent necessary to enable the CSRS to carry out its purpose in a reasonable manner.
>
> As previously stated, CSRS is responsible for providing security services for government buildings, employees, the judiciary, and members of government. CSRS used the Complainant's personal information for the sole purpose of assessing whether the Complainant's emails pose a hazard to ACPS employees and to either eliminate or control the hazard. Once a CSRS staff member determines the legitimacy of the email (relating to JSG programs and services), the Complainant's email is redirected to the appropriate program contact.

[para 9] The first question that must be addressed in a complaint regarding personal information is whether the information at issue is personal information. In this case, it would seem that the names of the Complainant's clients, in conjunction with the information that they have a matter in traffic Court would be personal information of the clients within the terms of section 1(n) of the FOIP Act. However, any information about

the Complainant in the request for disclosure would be about the Complainant acting in a representative capacity as the agent of his clients.

[para 10] Past orders of this office have held that information about a third party acting in a representative capacity, rather than a personal capacity, is not personal information within the terms of the FOIP Act. In Order F2013-51, the Director of Adjudication distinguished personal information from information about a third party acting as a representative. She said:

> As well, the Public Body has severed information, partly in reliance on section 17, that may be properly characterized as 'work product'. For example, it has severed the questions asked by an investigator, in addition to the answers of those interviewed. It has also withheld what is possibly a line of inquiry which the investigator means to follow (the note severed from record 1-151). While some of the questions and notes may reveal the personal information of witnesses, it does not appear that it is always the case that they do, and it appears possible that the Public Body withheld information on the basis that it may reveal something about the investigator performing duties on its behalf, rather than personal information about third parties.
>
> The Public Body has also withheld notes of an interview by the Public Body's investigator of the University of Calgary's legal counsel, in part in reliance on section 17. Information about the legal counsel's participation in the events surrounding the Applicant's complaint to the University is not her personal information unless it has a personal aspect, which was not shown.
>
> As well, it may be that some of the information of persons interviewed in the third volume relating to the Applicant's 'retaliation' complaint, which was withheld in reliance on section 17, may be information about events in which these persons participated in a representative rather than a personal capacity. Again, to be personal in such a context, information must be shown to have a personal dimension.
>
> In Order F2009-026, the Adjudicator said:
>
> > If information is about employees of a public body acting in a representative capacity the information is not personal information, as the employee is acting as an agent of a public body. As noted above, the definition of "third party" under the Act excludes a public body. In Order 99-032, the former Commissioner noted:
> >
> > > The Act applies to public bodies. However, public bodies are comprised of members, employees or officers, who act on behalf of public bodies. A public body can act only through those persons.
> >
> > In other words, the actions of employees acting as employees are the actions of a public body. Consequently, information about an employee acting on behalf of a public body is not information to which section 17 applies, as it is not the personal information of a third party. If, however, there is information of a personal character about an employee of a public body, then the provisions of section 17 may apply to the information. I must therefore consider whether the information about employees in the records at issue is about them acting on behalf of the Public Body, or is information conveying something personal about the employees.
>
> In that case, the Adjudicator found that information solely about an employee acting as a representative of a public body was information about the public body, and not information about the employee as an identifiable individual. In *Mount Royal University v. Carter*, 2011 ABQB 28 (CanLII), Wilson J. denied judicial review of Order F2009-026.

> In Order F2011-014, the Adjudicator concluded that the name and signature of a Commissioner for Oaths acting in that capacity was not personal information, as it was not information about the Commissioner for Oaths acting in her personal capacity. She said:
>
> > Personal information under the FOIP Act is information about an identifiable individual that is recorded in some form.
> >
> > However, individuals do not always act on their own behalf. Sometimes individuals may act on behalf of others, as an employee does when carrying out work duties for an employer. In other cases, an individual may hold a statutory office, and the actions of the individual may fulfill the functions of that statutory office. In such circumstances, information generated in performance of these roles may not necessarily be about the individual who performs them, but about the public body for whom the individual acts, or about the fulfillment of a statutory function.
>
> I find that the names and other information about employees of the Public Body and the University of Calgary acting in the course of their duties, as representatives of their employers, cannot be withheld as personal information, unless the information is at the same time that of an individual acting in the individual's personal capacity.

[para 11] From the foregoing, I conclude that information about a third party acting in a representative capacity will not be personal information, unless the information has a personal dimension. In cases where it is unclear from context that information has a personal dimension, it must be proven, with evidence, that the information has this quality.

[para 12] In this case, the information about the Complainant contained in the disclosure requests is information about the Complainant acting in a representative capacity. The complainant could not obtain the disclosure packages of another person from the Public Body for use in Court, unless he were representing the other person.

[para 13] I find that the information the Public Body's Corporate Security branch used was information about the Complainant acting in a solely representative capacity and lacked a personal dimension. As a result, I find that the Public Body's use of this information did not contravene Part 2 of the FOIP Act.

Issue D: Did the Public Body disclose the Complainant's personal information? If yes, did it do so in compliance with or in contravention of section 40 of the Act?

[para 14] As noted above, the Complainant complains that the Public Body included an email from the Corporate Security Branch to the Crown prosecution services branch that states:

> The attached Email is from [the Complainant] who is a known complex client to Corporate Security Services and his Emails has been re-directed for monitoring. There are times when [the Complainant's emails] are legitimate due to his current employment as a Traffic Ticket adviser and if the Email appears legitimate the Email will be forwarded for action. As indicated, the enclosed Email appears legitimate and is forwarded for your action.

I find that the statement indicating that the Complainant is a known complex client to Corporate Security Services and that his emails are redirected for monitoring is the personal information of the Complainant, as this statement does not refer to the Complainant in his representative capacity. Rather, the statement in the email that the Complainant is a "known complex client" is expressly contrasted to the Complainant's role as a Traffic Ticket adviser.

[para 15] From the email, one is able to conclude that the Complainant is "known" to the Corporate Security branch as a "client" and is considered complex or problematic in relation to his activities other than acting as an agent.

[para 16] It is not clear from the evidence whether the Complainant's clients viewed the information from Corporate Security Services that was included in the disclosure package. Regardless, I find that by including the email in a disclosure package intended to give the Complainant's clients the ability to respond to the Crown's evidence, the Public Body either disclosed the Complainant's personal information to the Complainant's clients, or created a situation in which it was likely that the Complainant's clients would view the information.

[para 17] Section 38 of the FOIP Act requires public bodies to protect personal information against various threats. It 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*

[para 18] Section 40 of the FOIP Act sets out the circumstances in which a Public Body is authorized to disclose personal information. The Public Body relies on sections 40(1)(x) and (ee) as authorization for disclosure of the Complainant's personal information.

> *40(1) A public body may disclose personal information only*
>
> *[…]*
>
> *(x) for the purpose of managing or administering personnel of the Government of Alberta or the public body,*
>
> *[…]*
>
> *(ee) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize*
>
> *(i) a risk of harm to the health or safety of a minor, or*
>
> *(ii) an imminent danger to the health or safety of any person […]*

[…]

(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.

[para 19] When I reviewed the Public Body's first set of submissions, I noticed that it had not made submissions addressing its inclusion of the Complainant's personal information in his clients' disclosure packages. I wrote the Public Body and stated the following:

> ln the background to the Notice of Inquiry, the complaint regarding disclosure is summarized in the following sentence: He [the Complainant] further states that Corporate Security Services has labelled him a "complex client", and that this information has been disclosed to third parties. In the Complainant's rebuttal submissions, he states:
>
> > Further, I wish to reiterate that it is a breach of my privacy to have emails relayed by me or on behalf of me be monitored and retained by the public body's corporate security, including having such disseminated to my clients through disclosure requests.
>
> I understand the Complainant complained that the Public Body included an email from its Corporate Security branch in a disclosure package intended for the Complainant's clients. This email states:
>
> > The attached Email is from [the Complainant] who is a known complex client to Corporate Security Services and his Emails has been re-directed for monitoring. There are times when [the Complainant's emails] are legitimate due to his current employment as a Traffic Ticket advisor and if the Email appears legitimate the Email will be forwarded for action. As indicated, the enclosed Email appears legitimate and is forwarded for your action.
>
> […]
>
> The Public Body has not made submissions regarding the disclosure that is the subject of the complaint or pointed to any authority to include communications of this kind in disclosure packages.

[para 20] Despite my request that the Public Body make submissions regarding its inclusion of emails from its Corporate Security Services branch, it did not make submissions on this point, or refer to any authority to do so. Instead, it stated:

> The Complainant's emails are redirected to CSS strictly in order to assess whether the correspondence is legitimate or if it may pose a security risk to GoA staff.
>
> The Public Body's obligation to ensure safety for its employees is authorized and mandated by the OHS Act and OHS Code. The Act specifically mandates that the employer protect staff from harassment and violence in the workplace. Parts 2 and 27 of the OHS Code speak specifically to managing risks associated with violence and harassment in the workplace and JSG's policies and procedures in this matter are in accordance with these requirements.

> Together, the OHS Act and OHS Code give the Public Body the express legal authority to use the Complainant's personal information in an effort to eliminate or control any potential hazard to GoA employees, which includes email redirect.

[para 21] The Public Body has not explained why including the email in a Crown disclosure package intended for the Complainant's clients would mitigate any risk posed by the Complainant.

[para 22] I have already determined that redirecting the Complainant's requests for disclosure on behalf of his clients to the Corporate Security Services branch does not engage the personal information protection provisions of the FOIP Act with regard to the Complainant's information, as any information about the Complainant is about him acting in a representative capacity. I accept that the Public Body had the purpose of managing employees when it redirected the email to the Corporate Security Services Branch. However, the information included in the disclosure package for the Complainant's clients is not the same information that was redirected. Rather, it is the Corporate Security Services branch's assessment of the Complainant as an identifiable individual.

[para 23] I find that the evidence does not establish that the Public Body had the purpose of managing employees when it included emails from the Corporate Security Services branch in the disclosure packages, given that the Public Body did not address this disclosure in its submissions, and because the disclosure to the Complainant's clients has no obvious relationship to the purpose of managing employees. Further there is no evidence before me that the head of the Public Body – the Minister of Justice and Solicitor General – formed the opinion that including the email in a disclosure package intended for the Complainant's clients would minimize a risk of danger to any person. As a result, section 40(1)(ee) has not been shown to authorize the disclosure.

[para 24] I have considered whether section 4(1)(k) would apply to the disclosure, given that disclosure packages are provided to the defense in prosecutions. Section 4(1)(k) states:

> *4(1) This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:*
>
> > *(k) a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed […]*

As the record in question (the email regarding the Corporate Security Services branch's reference to the Complainant as a "complex client") does not relate to a prosecution, I conclude that section 4(1)(k) does not apply to the disclosure.

[para 25] I am unable to find any authority under the FOIP Act for the inclusion of the Complainant's personal information in the disclosure package. As a result, I find that the Public Body contravened Part 2 of the FOIP Act when it included the email in the disclosure package. I make this finding on the basis that whether or not the

Complainant's clients actually viewed the email, the Public Body created a situation where it is likely that they would, and in doing so, contravened section 38 of the FOIP Act.

[para 26] I must therefore require the Public Body to ensure that it does not include emails referring to the Complainant as an identifiable individual in Crown disclosure packages in the future, unless there is authority under section 40 to do so.

IV. ORDER

[para 27] I make this Order under section 72 of the Act.

[para 28] I order the Public Body to cease including emails from its Corporate Security branch regarding the Complainant in disclosure packages unless it has authority under Part 2 of the FOIP Act to do so.

_____

Teresa Cunningham
Adjudicator
/ah