Order F07-10

THE BOARD OF EDUCATION OF SCHOOL DISTRICT NO. 75 (MISSION)

David Loukidelis, Information and Privacy Commissioner

June 26, 2007

Quicklaw Cite: [2007] B.C.I.P.C.D. No. 15
Document URL: http://www.oipc.bc.ca/orders/OrderF07-10.pdf

Summary: In 2004, the Board began requiring applicants for teaching positions to complete an on-line assessment developed and administered in the United States. The collection of personal information through the assessment is not expressly authorized by or under an Act, but it does, with the exception of social insurance numbers, relate directly to the Board's recruitment process for new teachers under s. 26(c) and is necessary. The Board made reasonable security arrangements for the protection of the personal information under s. 30. The complainants alleged the requirements of s. 30.1(a) were not met because the consent to storage and access outside Canada was not voluntary and did not meet the prescribed requirements for consent. The electronic form of consent was sufficient and there was no evidence that the consents were not voluntary. The use of the personal information for screening new applicants was consistent with the purpose for which it had been obtained under s. 32(a) and also met the consent requirement under s. 32(b).

Statutes Considered: B.C.: *Freedom of Information and Protection of Privacy Act*, ss. 26(c), 27, 30, 30.1, 32, 32(a) and 32(b). Freedom of Information and Protection of Privacy Regulation, B.C. Reg. 323/93, s. 6; *Personal Information Protection Act,* s. 7(2); *School Act,* ss.15, 15(1); *Workers' Compensation Act,* s. 31. **U.S.:** *USA Patriot Act, 2001*, Pub. L. No. 107-56, 115 Stat. 2135.

Authorities Considered: B.C.: Order F05-02, [2004] B.C.I.P.C.D. No. 2; Order No. 194-1997, [1997] B.C.I.P.C.D. No. 55; Order 02-38, [2002] B.C.I.P.C.D. No. 38; Order P05-01, [2005] B.C.I.P.C.D. No. 18; Order 04-19, [2004] B.C.I.P.C.D. No. 19; Order 00-47, [2000] B.C.I.P.C.D. No. 51; Investigation Report No. P97-009, [1997] B.C.I.P.C.D. No. 31. **Alta.:** Order 98-002, [1998] A.I.P.C.D. No. 18. **Ont.:** Investigation I94-004M, [1994] O.I.P.C. No. 457; Privacy Complaint MC-03044-1, [2004] O.I.P.C. No. 196.

Cases Considered: *Royal City Jewellers & Loans v. New Westminster (City)*, [2006] B.C.J. No. 270, 2006 BCSC 203; *Rizzo & Rizzo Shoes (Re)*, [1998] 1 S.C.R. 27; *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, 2002 SCC 53; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403; *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, [2004] S.C.J. No. 44; *Air BC Ltd. v. C.A.W.-Canada, Local 2213* (1997), 61 L.A.C. (4th) 406; *NorthwesTel Inc. and I.B.E.W., Loc. 1574, Re* (1996), 55 L.A.C. (4th) 57; *G., Re*, (1984), 51 Nfld. & P.E.I.R. 263 (Nfld. U.F.C.); *Société de transport de la Ville de Laval c. X*, [2003] J.Q. No. 1284, [2003] C.A.I. 664 (C.Q); *X. c. Résidence L'Oasis Fort-Saint-Louis*, [1995] C.A.I. 367; *X. c. Synergic International 1991 Inc.*, [1995] C.A.I. 361.

1.0 INTRODUCTION

[1] In 2004, The Board of Education of School District No. 75 (Mission)[1] ("Board") began using the "Gallup TeacherInsight Assessment" ("Assessment"), an on-line computer-based assessment tool developed and administered in the United States, to screen applicants for teaching positions. In 2005, the British Columbia Teachers' Federation ("BCTF") and the Mission Teachers' Union ("MTU") (collectively, "Complainants") filed a complaint with this office alleging that the Board's collection of personal information through the Assessment contravenes ss. 26, 30, 30.1 and 32 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

[2] Section 42(2)(e) provides authority to investigate and attempt to resolve complaints regarding the collection, use or disclosure of personal information in contravention of Part 3 of FIPPA. The matter was initially opened as an investigation under s. 42(2)(e) and attempts were made at mediation. For reasons that are not clear from the material before me, after mediation failed this office sent a Notice of Written Inquiry to the parties and gave notice to The Gallup Organization ("Gallup") under s. 54 of FIPPA. No objections were raised about proceeding by way of inquiry rather than investigation.

[3] Section 42(1)(b) of FIPPA provides that an order described in s. 58(3) may be made "whether the order results from an investigation or audit under paragraph (a) or an inquiry under section 56". I conclude that the inquiry process employed here, while it is not what is generally contemplated for Part 3 complaints, gave those involved a full opportunity to address the issues raised by the complaint and that the evidence filed provides a sufficient basis for making an order under s. 58(3).

[4] The Board did not raise the issue of standing, but it should be noted that the Complainants are organizations, not individuals, and are not directly affected by use of the Assessment. Part 3 deals with "personal information", which

[1] When the parties made their submissions the Board's corporate name was "The Board of School Trustees of School District No. 75 (Mission)". The name change reflected here was effected by s. 14 of the *School (Student Achievement Enabling) Amendment Act, 2007*.

Schedule 1 of FIPPA defines as "information about an identifiable individual other than contact information". FIPPA does not extend privacy protection to public bodies or organizations.[2] I accept, however, that it is appropriate to proceed with the inquiry in view of the serious issues that have been raised and the broad discretion under s. 42(1)(a) regardless of whether an individual has complained.

2.0 ISSUES

[5] The issues in this case are as follows:

1. Is the Board authorized to collect the personal information through the Assessment under s. 26 of FIPPA?;

2. Has the Board made reasonable security arrangements with respect to personal information collected through the Assessment under s. 30 of FIPPA?;

3. Has the Board obtained consent to storage and access of the personal information collected through the Assessment under s. 30.1(a) of FIPPA?; and

4. Is the Board's use of the personal information collected through the Assessment authorized under s. 32 of FIPPA?

[6] The initial complaint alleged that the Board's use of the Assessment contravened ss. 26, 30, 30.1 and 32 of FIPPA. While the Complainants stated, without elaboration, that other provisions governing personal information "may also have been violated", they indicated that the real issue was that the Board should not be "collecting" the information in the first place. The Complainants raised allegations concerning ss. 27, 33, 33.1 and 74.1 for the first time in their initial submission. The Board took the position that I should disregard the submissions in relation to these new sections as the Notice of Written Inquiry had limited the scope of the inquiry to ss. 26, 30, 30.1 and 32.

[7] I agree with the Board. While the Complainants alluded in the initial complaint to other FIPPA provisions that may have been violated, this was not, in my view, sufficient notice to raise new allegations, at the inquiry stage, respecting other FIPPA sections. The inquiry was convened in order to determine whether the requirement for applicants to complete the Assessment contravenes ss. 26, 30, 30.1 and 32 and as a result the Board did not fully address ss. 27, 33, 33.1 and 74.1 in its submissions. Nor was it required to do so.

[8] I do not intend to address the new allegations raised in the Complainants' initial submission beyond noting that many of these allegations appear to merely

[2] See, for example, Order F05-02, [2004] B.C.I.P.C.D. No. 2.

restate arguments advanced under ss. 26, 30, 30.1 and 32 and, to that extent, they would not have affected the outcome of this inquiry in any event.

[9] Section 57 of FIPPA is silent on the burden of proof in relation to ss. 26, 30, 30.1 and 32. This is not surprising, as s. 42 appears to contemplate that complaints under these provisions will proceed by way of an investigation rather than inquiry. The Complainants contend that the Board bears the burden of proof. They rely on Order No. 194-1997,[3] where Commissioner David Flaherty held that the public body bears the burden of proof in relation to s. 26. The Board relies on the Notice of Written Inquiry, which states that each party is obliged to submit information to justify its position under each of these sections.

[10] While a public body is expected, for all practical purposes, to provide evidence of compliance with Part 3 of FIPPA in the context of an investigation under s. 42, in my view, this does not equate with the imposition of a legal burden of proof. Where the legislation is silent, I do not accept that a formal burden of proof lies on either party. In Order 02-38,[4] I considered a similar issue in the context of section 25(1):

> [37] …Where an applicant has argued that s. 25(1) applies, it will be in the applicant's interests, in practical terms, to identify information in support of that contention. For example, although an applicant will not know the contents of requested records, she or he may well be in a position to establish that there is a clear public interest in the matter generally… In other words, an applicant will be obliged, as a matter of common sense, to provide evidence and explanation for her or his assertion that s. 25(1) requires disclosure. This practical obligation may obviously be constrained, however, by the fact that the applicant does not have access to the disputed information.
>
> [38] I agree that, since the head of a public body must apply s. 25(1) even where no access request has been made, the head has some obligation to consider whether it applies on the facts known to the head. Consistent with this view, where a public body has, for example, relied on s. 25(1) in disclosing a third party's personal information, without an access request, and the commissioner later investigates that disclosure under s. 42 of the Act in response to a complaint, it will be up to the public body, in practical terms, to provide an explanation, including relevant evidence, as to why s. 25(1) required it to disclose the information.
>
> [39] Section 4 of the Act creates a right of access, where an access request is made under s. 5, to parts of a record not excepted from disclosure (if the information that is excepted can reasonably be severed). By contrast, s. 25(1) requires a public body to disclose information where certain facts exist, regardless of whether an access request has been made. Section 25(1) either applies or it does not and in a Part 5 inquiry it is

[3] [1997] B.C.I.P.C.D. No. 55.
[4] [2002] B.C.I.P.C.D. No. 38.

> ultimately up to the commissioner to decide, in all the circumstances and on all of the evidence, whether or not it applies to particular information. Again, where an applicant argues that s. 25(1) applies, it will be in the applicant's interests, as a practical matter, to provide whatever evidence the applicant can that s. 25(1) applies. While there is no statutory burden on the public body to establish that s. 25(1) does *not* apply, it is obliged to respond to the commissioner's inquiry into the issue and it also has a practical incentive to assist with the s. 25(1) determination to the extent it can.

[11] In the absence of a statutory burden of proof, it is incumbent upon both parties to bring forward evidence in support of their positions, recognizing, of course, that I must ultimately determine whether or not there has been compliance with these provisions of FIPPA and that the public body is ordinarily best placed to offer evidence of its compliance.

[12] The Board submitted the substantive portion of the Assessment—*i.e.*, the Likert-type, multiple choice and open-ended questions—on an *in camera* basis because it is bound by certain confidentiality provisions in its Master Consulting Services Agreement with Gallup. The Board filed an affidavit from Lisa Kiichler, Vice President and Associate Counsel of Gallup, asserting that Gallup has intellectual property rights and copyright protection with respect to the questions contained in the Assessment. I accept that the material was properly received on an *in camera* basis because disclosure of this record would reveal information that may otherwise be protected from disclosure under s. 21.

3.0 DISCUSSION

[13] **3.1 Background**—The essential facts are not in dispute. The Board is established under the *School Act* to provide educational programs and services to approximately 7,200 students enrolled at public schools in the Mission school district. Each year, the Board receives approximately 300 unsolicited applications for teaching positions from external applicants and teachers on call (the latter are also known as substitute teachers). In October 2004, the Board began using the Assessment to screen applications from new applicants for teaching positions. At the time of the inquiry, Gallup, which is based in Omaha, Nebraska, provided the service to eight school districts in Canada.

[14] As part of its application screening process, the Board tells new applicants that they must complete the Assessment. Loris Pante is the Director of Human Resources for the Board. He deposed in his affidavit that the following letter is sent to new applicants:

> Dear applicant:
>
> We are currently reviewing all applications on file. As part of our application screening process, we require all applicants to take a web-based

> assessment called TeacherInsight. If you do not have access to the internet, contact Charlotte Thomas at 604-826-6286 Ext. 238 to make arrangements for doing the assessment at the School Board Office.
>
> - TeacherInsight will require approximately 40 - 45 minutes of uninterrupted time.
> - Log on the website by going to url http://gx.gallup.com/teacherinsight1.gx. You will be asked to enter a district code which is [*sic*].
> - You will be asked to provide your Social Insurance Number as the means for identifying yourself in the system. If you do not wish to use your SIN, contact Charlotte Thomas, as above, and she will contact the Gallup organization to request that they assign a code number to you.
> - TeacherInsight consists of multiple choice, Likert-type items (responses on a one-to-five scale) and open-ended items in which you write your response. The response time is preset, so be sure you are not being interrupted while doing the assessment.
> - Specific instructions are contained within the TeacherInsight.
>
> After completing the assessment you may be contacted for a personal interview dependent on our staffing requirements.

[15] There is some dispute in the evidence as to whether all applicants receive this letter. Dennis Keis, who is the President of the MTU, deposed in his affidavit that many teachers on call do not receive this form letter and are generally told by telephone that they are required to take the Assessment.

[16] After applicants receive notice that they must complete the Assessment, they must log on to the Gallup website to complete it. At the outset of that process, they are asked to provide the following information:

- a numeric code identifying the Board (this is required to access the Assessment site);
- their social insurance number or substitute numeric identifier; and
- their country of residence.

[17] If an applicant objects to providing his or her social insurance number, the Board will arrange for the assignment of a substitute numeric identifier.[5] After the applicant provides this initial information, the following screen appears:

[5] Mr. Keis indicates in his affidavit that he is aware of three teachers on call who were unaware that they had the option to provide substitute identifiers.

TeacherInsight Assessment

WELCOME PAGE:

(Name of School District) has asked Gallup to help in their recruiting and hiring process. We recognize that this may be the first time you have been asked to answer questions in this manner, and we appreciate your time and effort in doing something that may be new and unfamiliar.

The questions you will be asked are simple and straightforward. People who have responded to these questions have described them as thought provoking. The questions are grouped into three (3) sections. You will be given specific instructions at the start of each section.

The assessment will require approximately 45 minutes. You must complete the entire assessment in order for the district to receive your results. If you are interrupted or disconnected from the assessment, you may come back to the site and log in again. You will be returned to the point at which you left the assessment.

Your responses are confidential and will be recorded and analyzed by Gallup. Assessment results will be forwarded to the school district and used as one step in the hiring process.

The following assessment is copyrighted and may only be used with permission of The Gallup Organization. It is unlawful to record, copy, or reproduce the assessment in any form.

[18] The next screen contains a consent form in the following format:

DATA CONSENT PAGE:

The personal privacy laws of your country require that we obtain your consent before we continue. This assessment is being conducted for ***(School District Name)***'s hiring and recruiting purposes. We assure you that your responses to the assessment are completely confidential and your participation is voluntary. If you choose not to consent, you will not continue through the assessment. You also have the right to correct any errors in your personal data. The Gallup Organization will process all the information provided and may retain this information as part of a permanent database. Your personal data and responses will be processed in the United States.

CONSENT: Do you voluntarily agree and give your consent for Gallup to perform the activities described above and

consent to your data being transferred to the United States? ***[Radio buttons]***

1 I consent - **(Skip to Name Page)**
2 I do not grant consent - **(Decline)**

[19] If an applicant consents, the applicant is then asked to provide his or her name and contact information and then to respond to a series of multiple choice questions such as "What caused you to apply to this school district?" and "What was your initial contact with the school district?" The applicant is then asked to identify his or her first and second choices for grade and subject level and to confirm whether or not she or he is certified to teach in the Board's jurisdiction before the next school year. As indicated above, the substantive portion of the Assessment is divided into three sections comprised of Likert approach, multiple choice and open-ended questions.

[20] The information collected through the Assessment is stored in Gallup's database, which is located in Nebraska. Gallup uses the responses to prepare a report, which includes a numeric score that, Gallup claims, is predictive of an applicant's potential for teaching success in the classroom. The score is developed by comparing the applicant's responses to information in Gallup's research database. Gallup then reports the applicant's name and numeric score to the Board through its web-based reporting site, Gallup University Online, or transmits the score electronically. The Board uses the numeric score as one tool to assist it in short-listing a group of qualified candidates for interviews. Final selection decisions are based on personal interview results and reference checks.

[21] The MTU first raised concerns about the Board's use of the Assessment in early 2005. On March 3, 2005, the BCTF wrote to the Board urging the district to stop using the Assessment on the basis that it violates the privacy rights of applicants. On June 1, 2005, the BCTF declared the Board "in dispute" over the use of the Assessment. Under the BCTF's Code of Ethics, teachers are not to apply for or accept a position subject to an "in dispute" declaration.

[22] On June 3, 2005, the BCTF and MTU filed a grievance alleging that the Board's use of the Assessment to screen the applications of teachers on call violated the Provincial Collective Agreement. In August 2005, on behalf of the Board, the B.C. Public School Employers' Association applied to the British Columbia Labour Relations Board ("LRB") under s. 70 of the *Labour Relations Code* for, among other things, a declaration that the BCTF's "in dispute" declaration was void and unenforceable. At the LRB hearing, two teachers who applied for teaching positions in the district testified that they would have voluntarily completed the Assessment if the BCTF had withdrawn or rescinded the "in dispute" declaration. On September 7, 2005, the LRB granted the application in part and found that the "in dispute" declaration was void and unenforceable. On September 26, 2005, the BCTF applied for leave and

reconsideration of the LRB's decision on the basis of a constitutional challenge. On February 27, 2006, the LRB granted leave but dismissed the application for reconsideration.

[23] **3.2 Authority to Collect Personal Information**—Section 26, which places limits on the collection of personal information by or for a public body, reads as follows:

> **Purpose for which personal information may be collected**
>
> 26 No personal information may be collected by or for a public body unless
>
> (a) the collection of that information is expressly authorized by or under an Act,
>
> (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.

Parties' Arguments

[24] The Complainants contend that the names, social insurance numbers, contact information, and answers and scores of individuals constitute "personal information" as that term is defined in Schedule 1 of FIPPA. The Complainants argue that the collection of this personal information is not authorized by s. 26 because: (a) the collection of that information is not authorized by any Act; (b) the information is not being collected for the purposes of law enforcement; and (c) the information does not relate directly to nor is it necessary for an operating program or activity of the Board. In relation to s. 26(c), the Complainants contend that the Board must establish a "demonstrable need for the information such that the operating program or activity would not be viable without it". They argue that the Board cannot establish such a need as it has recruited and hired teachers for decades without resort to this tool. It also points out that other school districts continue to recruit teachers without using the Assessment.

[25] The Complainants also argue that s. 26 requires public bodies to collect the minimum amount of personal information that they require. While acknowledging that school districts must collect some personal information from applicants, the Complainants submit that the Board does not need to collect "personal psychological testing information" in order to select employees. The Complainants submit that the collection of social insurance numbers from applicants at the application stage also cannot be justified.[6]

[6] They cite in support Investigation Report No. P97-009, [1997] B.C.I.P.C.D. No. 31.

[26] There is no dispute that the information in question is "personal information" within the meaning of that term under Schedule 1. The Board acknowledges that it collects personal information but points out that all of the questions contained in the Assessment are questions that could be properly asked in an in-person interview. The fact that the information is collected electronically rather than in person does not, in the Board's submission, transform the questions and answers into "psychological information". The Board submits that s. 26(a) authorizes the collection of personal information in the Assessment because school boards are charged with responsibility for hiring staff under s. 15 of the *School Act.* It submits that the collection of information in the Assessment is logically and rationally connected to that ongoing purpose.

[27] The Board also contends that s. 26(c) authorizes the collection of personal information because the information is necessary for and relevant to the public body's activity of recruiting and selecting qualified employees. The Assessment enables the Board to screen a large volume of applications in an efficient and cost-effective way. The Board also believes strongly in the efficacy of this tool as a predictor of teacher success. The Board maintains that it has authority to determine what personal information is relevant and necessary with respect to recruitment and hiring criteria, particularly when the selection process involves a position of trust.

[28] No one has disputed that Gallup's collection of personal information through the Assessment, including answers to Assessment questions, is a collection of personal information by the Board. Nor is it contended that, because the Board does not receive individual candidates' answers to the questions, there is no collection of personal information in that respect.

[29] Section 26 recognizes the need for public bodies to collect personal information in order to carry out their mandates but restricts that collection to a defined set of circumstances. While some legislation expressly authorizes the collection of specific types of personal information, most statutes simply authorize programs or activities. Legislation which falls into this latter category would generally only provide implicit authority to collect personal information, which is not sufficient to meet the test under s. 26(a).[7]

[30] In support, the Board relies on a complaint investigation report from this Office that involved an allegation that the Insurance Corporation of British Columbia had contravened s. 26 by requiring applicants for driver's licences to provide information about their weight.[8] The complaint was dismissed because s. 25 of the *Motor Vehicle Act* expressly authorized the collection of information that would identify individuals to the satisfaction of the corporation. This decision does not assist the Board. Section 15(1) of the *School Act* simply says that

[7] Investigation Report P98-012 at URL: http://www.oipc.bc.ca/investigations/reports/invrpt12.html.
[8] http://www.oipc.bc.ca/orders/other_decisions/otherdec_3.html.

a "board may employ and is responsible for the management of those persons that the board considers necessary for the conduct of its operations". There is no language expressly authorizing or directing the collection of personal information for the hiring process. While it is implicit that the Board will have to collect personal information for the purpose of employing individuals, that does not meet the test under s. 26(a). If, as the Board contends, broad enabling language of this nature were sufficient to provide express authority for s. 26(a) purposes, there would be no need for s. 26(c) of FIPPA at all.[9]

[31] This leaves the question of whether the Board was authorized under s. 26(c) to collect personal information that relates directly to and is necessary for an operating program or activity of the Board. In the present case, I am satisfied that all of the personal information collected in the Assessment, with the exception of social insurance numbers, relates directly to the activity of recruiting and hiring teachers. Information concerning the qualifications, teaching preferences and aptitude of applicants is directly relevant to the task of finding qualified and suitable teachers and thus falls squarely within the Board's mandate under s. 15 of the *School Act*. The Board's collection of the personal information therefore meets the first part of s. 26(c), as it relates directly to the operating program or activity of recruitment and hiring of teachers.

[32] The remaining question under s. 26(c) is whether the personal information that the Board collects through the Assessment is "necessary" for the Board's operating program or activity of recruitment and hiring.

Reviewability of collection of personal information

[33] I do not accept the Board's contention that it has the final authority to determine what personal information is relevant and necessary. Although the Board makes the initial determination of what personal information it requires, its collection of personal information is subject to scrutiny through a complaint to this Office. This fact is not altered because, as the Board argues, the teacher hiring process involves filling positions of "trust".[10]

[34] The Board relies in this respect on a 2003 report of an investigation under the Alberta *Freedom of Information and Protection of Privacy Act*. That report concluded that the Calgary fire department's collection of personal information

---

[9] In saying this, I am aware of the decision of in *Royal City Jewellers & Loans v. New Westminster (City)*, [2006] B.C.J. No. 270, 2006 BCSC 203. In that case, Boyd J. held that reference in s. 26(a) to collection of personal information authorized by or "under an Act" encompassed cases where *Community Charter* authority exists to enact a bylaw compelling information to be provided. She held that the *Community Charter* is an Act that authorizes the bylaw under attack, which in turn expressly compelled the provision of information. This decision is under appeal to the Court of Appeal and judgement is awaited at this time. This decision does not in any case support the Board's position respecting s. 26(a), since the *Community Charter* section in question explicitly authorizes a bylaw to be enacted that compels "information".

[10] Para. 33, initial submission.

from firefighter candidates through a personal history disclosure form was authorized under the Alberta equivalent of s. 26(c).[11] The form asked candidates to disclose, among other things, "detected" and "undetected" criminal activity. The report said the following about this collection of personal information:

> [14] In Order 98-002 [para 181], the Commissioner said the decision as to what personal information is relevant and necessary rests with the "decision maker". The Commissioner said he would give public bodies "considerable latitude" in this determination and that he would most likely not interfere provided the determination is not patently unreasonable. The requirement of reasonableness in relation to section 33(c) of the FOIP Act was reiterated in Order 2001-034 [para. 21].

[35] In Alberta Order 98-002,[12] Commissioner Bob Clark had to decide whether the Alberta Workers' Compensation Board ("WCB") could collect personal information because it was "necessary" within the meaning of s. 33(c) of Alberta's *Freedom of Information and Protection of Privacy Act*. I note that s. 31 of the *Workers' Compensation Act* explicitly authorized the WCB to collect personal information "relative to the disability and compensation" of a worker "that it considers necessary". Commissioner Clark in light of this explicit statutory authority for the WCB to collect what it "considers necessary" went on to interpret s. 31 as giving the WCB the "discretion to decide what information is necessary, relative to the disability and compensation." Immediately after noting this feature of the *Workers' Compensation Act*, Commissioner Clark went on to say, as noted in the Calgary fire department report, that he must give the WCB "considerable latitude" in deciding what personal information was necessary, adding that as long as the WCB's "determination is not patently unreasonable, it is not likely I would interfere." He concluded that, although he could not "defer entirely" to the WCB, he would not interfere with the WCB's determination if it "had a reasonable basis for deciding that the collection of the personal information was necessary, "relative to the disability and compensation."[13]

[36] To the extent this decision holds or suggests that a public body's decision to collect personal information will receive deference if there is a reasonable basis for deciding the information is necessary, or will receive deference unless that decision is shown to be patently unreasonable, I respectfully disagree. Public bodies require latitude in determining what personal information is necessary to effectively carry out their operating programs or activities, but s. 26(c) entirely delimits that latitude and a public body's actions are fully reviewable under FIPPA.

---

[11] Report on Investigation Regarding Collection, Use and Disclosure of Personal Information (City of Calgary – Calgary Fire Department): http://www.oipc.ab.ca/ims/client/upload/ACF7C3E.pdf.
[12] [1998] A.I.P.C.D. No. 18.
[13] Paras. 149-153.

What does "necessary" mean?

[37] Turning to s. 26(c), what meaning did the Legislature intend the word "necessary" to have?

[38] In interpreting FIPPA, its language is to be read in its grammatical and ordinary sense and its entire context, in harmony with FIPPA's scheme, its objective and the intention of the Legislature.[14]

[39] Section 2(1) articulates FIPPA's purposes. They are to make public bodies "more accountable to the public" and to "protect personal privacy". FIPPA's privacy protection goal is achieved, among other things, "by preventing the unauthorized collection, use or disclosure of personal information by public bodies".[15]

[40] Turning to the meaning of "necessary" in s. 26(c), the Supreme Court of Canada has said that, consistent with general interpretive principles, the meaning of "necessary" depends on its legislative context:[16]

> [91] The words of s. 2.4(1)(b) [of the federal *Copyright* Act] must be read in their ordinary and grammatical sense in the proper context. "Necessary" is a word whose meaning varies somewhat with the context. The word, according to *Black's Law Dictionary*,
>
> > … may mean something which in the accomplishment of a given object cannot be dispensed with, or it may mean something reasonably useful and proper, and of greater or lesser benefit or convenience, and its force and meaning must be determined with relation to the particular object sought. [Emphasis added by Binnie J.]

[41] The following complete quote from the *Black's Law Dictionary* (6th ed.) definition of "necessary" emphasizes the contextual malleability of "necessary", a word that is fairly common in statutes:

> This word must be considered in the connection in which it is used, as it is a word susceptible of various meanings. It may import absolute physical necessity or inevitability, or it may import that which is only convenient, useful, appropriate, suitable, proper, or conducive to the end sought. It is an adjective expressing degrees, and may express mere convenience or that which is indispensable or an absolute physical necessity. It may mean something which in the accomplishment of a given object cannot be dispensed with, or it may mean something reasonably useful and proper,

---

[14] See, for example, *Rizzo & Rizzo Shoes (Re)*, [1998] 1 S.C.R. 27, applied in, for example, Order 02-38, [2002] O.I.P.C.D. No. 38. Also see s. 8 of the *Interpretation Act*.
[15] FIPPA, s. 2(1)(d).
[16] *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, [2004] S.C.J. No. 44, Binnie J.

> and of greater or lesser benefit or convenience, and its force and meaning must be determined with relation to the particular object sought.[17]

[42] Decisions under similar Canadian privacy laws reflect a range of approaches in interpreting the word "necessary" as it governs personal information collection.

[43] Under Ontario's *Freedom of Information and Protection of Privacy Act* and its municipal equivalent, the *Municipal Freedom of Information and Protection of Privacy Act*, various approaches have been taken over the years. Some decisions apply a reasonableness standard while others indicate that collection and use of personal information is necessary only if there is no other alternative for the public body. An example of the latter approach is Investigation I94-004M, where then Assistant Commissioner, and now Commissioner, Cavoukian said this about a school board's collection of a grade eight student's name and address for the purpose of contacting her and her parents about secondary school registration:

> It is our view that since there existed an alternative way for the Board to notify prospective students and their parents without collecting the names and addresses of the students, the Board's collection of the complainants' daughter's personal information cannot be said to have been "necessary" to the Board's activity of notification of its programs and accommodation. Thus, in our view, the Board's collection was not in accordance with section 28(2) of the Act. [18]

[44] In Privacy Complaint MC-03044-1,[19] a housing corporation had required residents to provide a valid motor vehicle insurance certificate in order to park on site. This personal information was held not to be necessary to properly administer the parking program.

[45] I have considered the meaning of "necessary" in the context of British Columbia's *Personal Information Protection Act* ("PIPA"). In Order P05-01[20] I considered PIPA's explicitly-stated legislative purposes and concluded that the word "necessary" in s. 7(2) of PIPA meant personal information that is indispensable "in the sense that it is not possible to supply a product or service without the personal information or because it is legally required for the supply."[21] I acknowledged that there will "be cases where personal information is 'necessary' even though it is not, when considered in a searching yet reasonable

---

[17] *Air BC Ltd. v. C.A.W.-Canada, Local 2213* (1997), 61 L.A.C. (4th) 406 (McPhillips), p. 423, quoting from Black's Law Dictionary (6th ed.) at p. 1029. Also see, to similar effect, *NorthwesTel Inc. and I.B.E.W., Loc. 1574, Re* (1996), 55 L.A.C. (4th) 57 (S. Kelleher Q.C.), p. 73, and *G., Re*, (1984), 51 Nfld. & P.E.I.R. 263 (Nfld. U.F.C.), p. 267.
[18] [1994] O.I.P.C. No. 457, at p. 4.
[19] [2004] O.I.P.C. No. 196.
[20] [2005] B.C.I.P.C.D. No. 18.
[21] Para. 78.

manner, indispensable in the sense that it is not possible to supply the product or service without the personal information."[22] In concluding that the personal information that the organization involved had collected was "necessary", I considered three factors. The first was the sensitivity of the personal information (it was non-sensitive identifying information); the second was the particular purpose for the collection (the legitimate business purpose of fraud prevention); and the third was that the organization collected only the personal information that was directly related to and minimally required to achieve its legitimate purposes.[23]

[46] A single, rigid interpretation of the concept of necessity was questioned, in the context of personal information collection, by Filion J. in *Société de transport de la Ville de Laval c. X*: [24]

> …[It is] unproductive to tie oneself to a fixed definition of necessity and to a technical application of that one criterion, without considering the particular facts of each case, the type and the nature of the information in issue and the objectives pursued by the organization. Accordingly, the interpretation should permit a more dynamic criterion, one that is more accurate and also better suited to evaluation of the merits of each case.
>
> …
>
> …It is not a question of determining what necessity is in itself so much as deciding, in the context of the protection of personal information, and for each case, what is necessary for the accomplishment of each particular purpose...[25]

[47] A relevant part of the interpretive context of s. 26(c) and FIPPA overall is the reality that governments need personal information to do their work. They cannot provide services, confer benefits or regulate conduct without our personal information. For this reason, citizens may be compelled by law to give up their personal information or will disclose it to receive services or benefits and one cannot ignore the power of the state in relation to personal information collection in interpreting what is meant by "necessary" in s. 26(c).

[48] The collection of personal information by state actors covered by FIPPA—including local public bodies such as the Board—will be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of FIPPA. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.

---

[22] Para. 78.
[23] Paras. 87-89.
[24] [2003] J.Q. No. 1284, [2003] C.A.I. 664 (C.Q), paras. 30 and 33. My translation.
[25] Para. 33.

[49] At the same time, I am not prepared to accept, as the Complainants contend, that in all cases personal information should be found to be "necessary" only where it would be impossible to operate a program or carry on an activity without the personal information. There may be cases where personal information is "necessary" even where it is not indispensable in this sense. The assessment of whether personal information is "necessary" will be conducted in a searching and rigorous way. In assessing whether personal information is "necessary", one considers the sensitivity of the personal information, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purpose for collection. In addition, FIPPA's privacy protection objective is also relevant in assessing necessity, noting that this statutory objective is consistent with the internationally recognized principle of limited collection.

[50] Viewed in this light, is the Board's collection of personal information through the Assessment "necessary"?

[51] The Complainants cite the provincial government's manual on FIPPA in support of their contention that the personal information collected through the Assessment is not "necessary" for the Board's hiring activities. They say this:

> Given that the School District has recruited and hired teachers for decades without the use of the information in the Assessment/Assessment scores, and that other school districts are able to do so, it cannot establish that this personal information is necessary to its hiring activity, or that the School District's hiring activity would not be available without the Assessment.[26]

[52] While they acknowledge that the Board must collect some personal information from applicants, the Complainants say it does not "need to collect psychological testing information" to do so[27] and is "collecting far more personal information than required for hiring purposes."[28]

[53] The evidence before me does indicate that only seven other school districts in Canada use the Assessment. While it is thus reasonable to infer that other school districts are able to use more traditional methods to screen teacher applications, I do not place a great deal of weight on this. It may be that the Board is on the leading edge of recruitment methods and is an early adopter of a method that other school districts, if not other employers, have yet to exploit.

[54] The Assessment uses current information technology to collect personal information and produce information that is, according to the Board, a useful, but not the only tool, it employs to assess job applicants. The Board submitted

[26] Para. 34, initial submission.
[27] Para. 35, initial submission.
[28] Para. 39, initial submission.

evidence that the Assessment scores assist the Board in screening a large number of applicants quickly and cost-effectively. There is evidence that the Assessment identifies applicants who have the knowledge, skills and abilities similar to those of the best teachers. It is said that this assists the Board in focussing its resources on personally interviewing and assessing candidates and making selection decisions.[29]

[55] The Complainants have a copy of the Assessment. They contend that the Board is collecting "far more personal information than required for hiring purposes"[30] and characterize the Assessment and resulting scores as "psychological testing information"[31] and "psychological profiling".[32]

[56] Certainly, questions in the Assessment draw out individuals' attitudes about the nature of teaching, ascertain how they would react to certain scenarios in the classroom or with their teaching colleagues, elicits how they perceive themselves in terms of attributes such as honesty and emotional control, and draws out how they believe others see them.[33] To some extent, one could say the answers, and the scores that Gallup assigns and reports to the Board, applying the results of Gallup's research methods, reveal something about the 'psychological' makeup of respondents. Put another way, however, it is reasonable to infer that the Assessment tells the Board something about the character and aptitude of those who apply to teach children for whose education the Board is responsible.

[57] I take notice of the fact that employers—including this Office—may ask questions intended to elicit information about candidates' character and aptitude for the position and that the Assessment includes questions much like those one encounters during face-to-face job interviews. Employers may ask questions similar to those found in the Assessment, although this may be done during face-to-face interviews (perhaps with applicants who have passed first-cut screening of some kind). Even using this method, candidates' answers will be noted and assessed by the employer or its consultants, enabling the employer to assess and rank, with varying degrees of formality, competing candidates' competencies across a range of job and personality attributes.

[58] The Complainants assert that necessity cannot be established because the Board has managed for decades to hire without using the Assessment. This assumes that the Board has not, in the past, collected personal information

---

[29] The Board's evidence is in the Affidavit of Lisa Kiichler, para. 10. Although she is employed by Gallup, which has an interest in the matter, it is appropriate to give weight to her evidence of utility and efficacy.
[30] Para. 35, initial submission.
[31] Para. 35, initial submission.
[32] Para. 11, initial submission.
[33] Some of these kinds of question are reproduced in para. 10 of the Complainant's initial submission.

similar to or essentially the same as that collected through the Assessment. The above observation that employers may collect similar personal information through more traditional selection methods does not prove necessity in this case, of course, but it does illustrate that the Complainants' position assumes something about the Board's past hiring practices that is not proven. Assuming for discussion purposes that the Board in the past did collect personal information such as that involved here, I would not find that objectionable for s. 26(c) purposes. Moreover, as noted earlier, the evidence offered by the Board is that the Assessment confers advantages that go beyond those available using more traditional, labour-intensive selection methods that entail collection of the same or similar personal information.

[59] I have decided after careful consideration that s. 26(c) authorizes the Board to collect the personal information that it collects through use of the Assessment. In arriving at this conclusion, I have considered the nature and extent of the personal information generated by the Assessment, the sensitivity of the information and the Board's purpose for collection. This conclusion, of course, is case-specific.

[60] As regards social insurance numbers, I do not accept that their collection relates directly to and is necessary for the screening process for external applicants such that their non-consensual collection is authorized. I agree with Commissioner Flaherty's observation in Investigation Report 97-009 that social insurance numbers are sensitive personal information because of their power to identify.[34]

[61] Social insurance numbers are only required for the purposes of federal programs such as income taxation and employment insurance. An employer is required to collect the social insurance numbers of employees for such programs, but it need not collect them from mere job applicants. This personal information cannot be said to be related directly to and necessary, within the meaning of s. 26(c), for the hiring process at the stage of processing or considering applications.

[62] I find that the collection of social insurance numbers from job applicants at the hiring or employment suitability assessment stage contravenes s. 26(c) and

[34] This is notably so because they are powerful tools for acquiring other personal information necessary to commit identity theft and fraud.

make the appropriate order below.[35] In this respect, I agree with rulings to the same effect of Quebec's Commission d'accès à l'information.[36]

[63] **3.3 Protection of Personal Information**—Section 30 imposes a duty on public bodies to protect personal information in their custody or under their control:

> **Protection of personal information**
>
> 30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[64] The Complainants contend that the Board has contravened s. 30 because it has not provided any assurances that Gallup is in compliance with FIPPA's requirements for retention, storage and disposal of personal information. The Complainants note that Gallup's Privacy Statement acknowledges the importance of the protection of personal information but falls short of setting out the protections that this Office has recommended in various reports and publications, such as the Guidelines for Data Service Contracts.[37] The Complainants contend that the personal information gathered in the Assessment is not granted the same level of protection in the United States where it is subject to the *USA Patriot Act*[38] and other laws.

[65] The Board acknowledges that its duty to ensure that reasonable security arrangements are in place extends to its service-providers such as Gallup. It maintains that Gallup has instituted a number of security arrangements to protect applicants' personal information from unauthorized access, collection, use, disclosure or disposal. The Board refers to Gallup's Privacy Statement and provisions in the Master Consulting Services Agreement, which provide that Gallup must not disclose personal information to third parties (including clients and other research organizations), with this obligation including the identity of individual respondents and any respondent-identifying information unless the respondent expressly consents to the disclosure of that information. The Board states that Gallup maintains a range of security safeguards, standards, policies

---

[35] I note in passing only that, after inquiry submissions were made, the School District provided affidavit evidence that, after a date specified in the affidavit, Gallup's system would no longer permit applicants to provide a social insurance number or other numeric identifier. The applicants requested an opportunity to respond to this further affidavit if I were to consider it in reaching my decision here. I have not considered this evidence in reaching my decision or making the related order under s. 58.

[36] See *X. c. Résidence L'Oasis Fort-Saint-Louis*, [1995] C.A.I. 367, and *X. c. Synergic International1991 Inc.*, [1995] C.A.I. 361.

[37] OIPC Guideline 01-02, http://www.oipc.bc.ca/advice/Guidelines-Data_services.pdf.

[38] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), 2001*, Pub. L. No. 107-56, 115 Stat. 2135.

and procedures which are designed to protect confidential data in its custody, as outlined in "Gallup's Data Security Safeguards and Procedures".

[66] The Board submits that it has discharged its duty to protect personal information under s. 30 through contractual provisions governing confidentiality under the Master Consulting Services Agreement and the privacy practices and security safeguards that Gallup has instituted. For its part, Gallup says it seeks the consent of every individual participating in any survey or assessment where the data is being gathered outside of the United States. Gallup states that all of its contracts contain language that state that the identity of an individual and his or her responses will not be disclosed without the express consent of the individual. Gallup also points out that any data that contains identifying information must be transferred using a secure, encrypted protocol.

[67] The Board argues that the risk of disclosure under the *USA Patriot Act* is minimal at best. It points out that the United States government would first have to know of the existence and location of the personal information in Gallup's database and secondly that the information would have to be of a type that would be likely to fall within the scope of what that Act is designed to discover. The Board suggests that the nature of the information stored by Gallup is quite remote from the type of information that might be the subject of court orders for disclosure of information "for foreign intelligence purposes or to protect against international terrorism or clandestine intelligence activities" under the *USA Patriot Act*. The Board expresses the opinion that it is highly unlikely that a research company such as Gallup would be the first or preferred source of such information.

[68] Gallup says it has not been subject to any orders under the *USA Patriot Act* to date, although how it can say this is unclear, since United States federal law prohibits anyone who has been the subject of such a court order, or a subpoena, from disclosing that fact.[39] While acknowledging such an order is technically possible, the Board maintains that Gallup would have a strong interest in defending the confidentiality of its proprietary information and would vigorously defend its position. The Board also argues that the name and contact information of applicants is often publicly available through sources such as telephone directories.

[69] The s. 30 requirement to make reasonable security arrangements does not foreclose the possibility of contracting out services involving the collection, use, storage and disclosure of such information.[40] Although public bodies can contract out services, it is well established that they cannot contract out of their

[39] 50 U.S.C. § 1861. Also see 18 U.S.C. § 2709(c).

[40] See, for example, Investigation Report 02-01, http://www.oipc.bc.ca/investigations/reports/IR02-01.pdf. Also see the OIPC's report, *Privacy and the USA Patriot Act—Implications for British Columbia Public Sector Outsourcing* (October 2004), p. 100. http://www.oipc.bc.ca/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final.pdf.

privacy obligations under FIPPA.[41] As was observed in this Office's report on the *USA Patriot Act*:

> …A public body cannot contract out of FOIPPA [FIPPA] either directly or by outsourcing its functions. The decision to outsource does not change the public body's responsibilities under FOIPPA. Nor does it change public and individual rights in FOIPPA, which are not balanced against any 'right' to outsource.
>
> Section 30 requires public bodies to make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information. When a public body contracts out functions, it must ensure there will be reasonable security arrangements for the personal information that it discloses to the contract and that the contractor collect or generates in fulfilling the outsourced function. The public body's responsibilities under section 30, and the required standard of security, are constants, with or without outsourcing.[42]

[70] The mere fact that a public body enters into a contract with a service provider does not contravene s. 30. The public body must, however, ensure that the service provider is contractually required to have standards and policies in place to provide the level of security required under Part 3 of FIPPA. In assessing the "reasonableness" of the security arrangements, consideration must be given to the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure.

[71] The Complainants say that the Board has failed to provide them with any assurances that Gallup is complying with FIPPA or that its contract with Gallup requires compliance with FIPPA. The Complainants do not, however, have privacy interests that are directly affected by the use of the Assessment. On this basis alone, the Board is not obliged to provide the Complainants with any assurances concerning its compliance with Part 3 of FIPPA.

[72] The Complainants point out that the Master Consulting Services Agreement does not contain all of the provisions suggested in OIPC Guideline 01-02, Guidelines for Data Services Contracts.[43] Even assuming the relevance of this guideline to the situation at hand, this does not in itself establish a contravention of s. 30. The guideline is just that—a guideline to assist public bodies in meeting their FIPPA obligations—and by its own terms it recognizes that the complexity of contractual arrangements varies depending on the nature of the personal information in question and the nature of the services to be provided. It is within a public body's discretion to decide which if any of the

---

[41] Order 04-19, [2004] B.C.I.P.C.D. No. 19; Order 00-47, [2000] B.C.I.P.C.D. No. 51; Investigation Report 02-01.
[42] *Privacy and the USA Patriot Act—Implications for British Columbia Public Sector Outsourcing*, above, at p. 100.
[43] http://www.oipc.bc.ca/advice/Guidelines-Data_services.pdf.

provisions in the guideline it will implement having regard to these considerations.

[73] The work to be performed under the Master Consulting Services Agreement between the Board and Gallup is set out in a Statement of Work which is not in evidence before me, but I note that the agreement itself contains detailed provisions protecting the confidentiality of any individuals who elect to participate in the Assessment. Clause 3.6 of the agreement clearly sets out that Gallup cannot disclose the identity of individual respondents or any respondent-identifying information unless the respondent expressly agrees to such disclosure. Gallup has appointed a Privacy Policy Administrator to monitor privacy practices within that organization. Employee access to information is restricted to a need-to-know basis. Gallup's Data Security Safeguards and Procedures provide detailed information on the steps that have been implemented to secure personal information. These steps involve password protection, measures to prevent outside unauthorized electronic access, file transfer protocols, protected storage and network access monitoring. All of these steps reflect that reasonable security arrangements have been made to guard against the risks of unauthorized access, collection, use, disclosure or disposal of personal information.

[74] In the absence of evidence establishing that the Board has failed to make reasonable security arrangements, there is no basis for finding that the Board has contravened the requirements of s. 30.

[75] This said, I will say that Gallup is strongly advised to implement measures to ensure that the identities of individuals who take the Assessment are not stored in its databases after Gallup has reported to the Board. Once an applicant has registered and completed the Assessment, I see nothing to prevent Gallup from assigning a unique numerical identifier to the individual, while stripping away the identity. In fact, the best approach would be for Gallup's clients to hold the key for associating the assigned identifier with the applicant's names, which would be in the clients' hands, not Gallup's. This would further improve information security for applicants, including in light of concerns raised about storage of the information outside Canada.

[76] **3.4 Storage and Access in Canada**—Section 30.1 of FIPPA provides that a public body must ensure that personal information in its custody or under its control is only stored and accessible in Canada unless one of three exceptions apply:

> **Storage and access must be in Canada**
>
> 30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

> (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;
>
> (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;
>
> (c) if it was disclosed under section 33.1(1)(i.1).

[77] The Complainants allege that the Board has violated s. 30.1 because the storage of and access to the personal information of applicants is in the United States and the exceptions do not apply. The Complainants submit that the Board cannot rely on s. 30.1(a) because the consent by applicants provided is compelled or coerced and therefore not valid:

> Before starting the Assessment, an applicant is asked whether they will consent to their personal "data" being transferred, processed and retained in the United States. The applicant may refuse to consent, but the Assessment will then terminate. The School District has made it clear that it will only consider applicants who have completed the Assessment. The applicant is in an untenable situation: if they want to be considered for the teaching position they must take the Assessment. Therefore, they must consent.[44]

[78] The Complainants also point out that s. 30.1(a) requires consent "in the prescribed manner". Section 6 of the Freedom of Information and Protection of Privacy Regulation ("FOI Regulation")[45] provides as follows:

> 6. The consent of an individual to a public body disclosing any of the individual's personal information under section 33(b) of the Act must
>
> (a) be in writing, and
>
> (b) specify to whom the personal information may be disclosed and how the personal information may be used.

[79] The Complainants say that the electronic form of consent provided online through the Assessment—by clicking an "I consent" button—does not constitute consent "in writing". They also argue that the consent does not specify to whom the personal information may be disclosed or how it may be used. While the Complainants acknowledge that the Board may be able to craft a written consent form that addresses the prescribed requirements, it submits that requiring a job applicant to complete the Assessment as part of the recruitment process can never result in voluntary consent.

---

[44] Para. 48, Complainant's initial submission.
[45] B.C. Reg. 323/93.

[80] The Board maintains that applicants provide valid consent. It submits that the legislative intent underlying s. 30.1(a) is the right of individuals to choose voluntarily to authorize disclosure, access and storage of their own personal information outside of Canada. This, it says, is precisely what occurs when a new applicant consents to participate in the Assessment.

[81] The Board submits that the consent provided by applicants is valid because it is both "voluntary" and "informed". It argues that the consent is voluntary because the applicants are educated professionals who are capable of deciding whether or not to answer questions that relate to their privacy rights. The Board suggests that to say that applicants are forced to consent because they want teaching positions is analogous to saying that a person who consents to surgery is being "forced" to consent to medical treatment because they want to be well. The Board argues that many choices affecting one's privacy are made on the basis of achieving a desired objective. It also points out that there is no evidence in this case that individuals failed to provide valid consent.

[82] The Board submits that the consent is "informed" because the purpose of collecting the information is identified at the outset of the assessment (*i.e.*, the information is collected for the Board's hiring and recruiting process). It claims that applicants are provided with sufficient information about the purposes for which the information is collected and how it will be used to make an informed choice about whether or not to participate in the assessment.

[83] There is no question that the personal information contained in the Assessments is stored in and accessible in the United States. The Board's opinion about the risk of disclosure under the *USA Patriot Act* is not relevant. The determination of whether the Board contravened s. 30.1 stands or falls on the validity of the consent provided by applicants. The question is whether applicants have provided valid consent, in the prescribed manner, to having their personal information stored and accessible outside Canada in accordance with s. 30.1(a).

[84] As a matter of law, there is no question that consent, to be validly given, must be voluntary and informed.[46] In this case, there is not sufficient evidence before me to establish that applicants who provided consent were coerced or forced to do so. Dennis Keis deposed that approximately 40 to 50 candidates for teaching positions have contacted the union since the fall of 2004 to raise concerns or questions about the requirement to complete the Assessment. He notes that some of the teachers on call were upset or angry about the requirement to take the Assessment. This evidence, in my view, falls short of

[46] For example, the courts have, in certain cases, held that consent will be legally ineffective if it can be shown that there was such a disparity in the relative positions of the parties that the weaker party was subject to exploitation because he or she was not in a position to choose freely, thus rendering the consent involuntary. See, for example, *Norberg v. Wynrib,* [1992] 2 S.C.R. 226.

establishing coercion or compulsion on the part of the Board respecting the consent issue at hand.

[85] I note in passing that, as indicated earlier, there will be cases where, in order to receive services or benefits from a public body, an individual is compelled to provide personal information or to permit it to be compiled. Many choices affecting one's privacy are made on the basis of achieving a desired objective and this holds true in dealings with public bodies as with private sector organizations. One might prefer to choose not to provide government with, or permit it to compile, personal information that enables it to assess and collect income taxes that pay for public services, but that choice is not on offer.

[86] The remaining question is whether the electronic form of consent meets the requirements under s. 6 of the Regulation. Section 6 provides that: (a) the consent must be in writing; (b) the consent must specify to whom the personal information may be disclosed; and (c) the consent must specify how the personal information may be used.

[87] On the first issue, I accept that an electronic form of consent is valid by virtue of s. 5 of the *Electronic Transactions Act*, which reads as follows:

> 5 A requirement under law that a record be in writing is satisfied if the record is
>
> (a) in electronic form, and
>
> (b) accessible in a manner usable for subsequent reference.

[88] The requirement of consent "in writing" in s. 6(a) of the FOI Regulation is a "requirement under law" to which s. 5 of the *Electronic Transactions Act* applies.

[89] I also accept that the data consent page and the introductory page of the Assessment together provide enough information to enable applicants to provide informed consent. These pages specify to whom the personal information may be disclosed (Gallup has identified that personal information will only be disclosed to the Board and will otherwise remain confidential) and outline how the personal information may be used (it will be recorded and analyzed by Gallup in the United States, assessment results will be forwarded to the Board for use as one step of its hiring process and the data may be retained as part of a permanent database in the United States). It is critical to my finding that the consent form provides explicit notice to applicants that their personal information will be stored and accessed in the United States.

[90] I will add here, in passing, that a public body such as the Board using a form of electronic consent should ensure that it is in a position later to establish

that the consent was given. A traditional written consent can be demonstrated by producing the original or a proven copy of the signature of the individual, but this is not feasible at this time with an electronic consent such as that used by the Board.[47] Here, the evidence shows that an individual cannot proceed beyond the consent page unless she or he clicks the "I consent" button. This suffices and public bodies should ensure that they are able to provide similar or other evidence in such cases.

[91] To summarize, I agree with the Board that there is no evidence to establish that there has been any compulsion or coercion on its part or on the part of Gallup in obtaining consent from applicants who have completed the Assessment. I am satisfied that the introductory and data consent pages of the Assessment meet the consent requirements of s. 6 of the FOI Regulation. I therefore find that the Board has met the requirements under s. 30.1(a) to permit storage and access to personal information outside Canada.

[92] **3.5 Use of Personal Information**—Section 32 requires a public body to ensure that personal information in its custody or under its control is used only in accordance with the limits imposed under that section:

> **Use of personal information**
>
> 32 A public body must ensure that personal information in its custody or under its control is used only
>
> (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),
>
> (b) if the individual the information is about has identified the information and has 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 sections 33 to 36.

[93] The Complainants allege that the Board's use of personal information collected from the Assessment violates s. 32 of the Act. While applicants are notified that the personal information is used for the hiring and recruitment process, the Complainants say that the personal information is also used for a number of purposes that are not disclosed, such as:

- used to assess the applicant's teaching and psychological suitability;
- used to provide the applicant with a score as a percentile;
- used to screen out applicants at the School District's offices;
- used to validate Gallup's assessment;

[47] Although increasingly common, digital signatures are not yet in widespread use such that they will address this issue in the near term.

- used where the U.S. government seeks the information pursuant to the *Patriot Act;*
- stored indefinitely; and/or
- transferred to a third party contractor.[48]

[94] According to the Complainants, none of these is a use "for which the personal information was obtained and they are not uses that the Board or Gallup advised the applicant of". The Complainants argue that these uses do not meet the definition of "consistent purpose" within the meaning of s. 34 because there is no logical and plausible link between hiring and many of the purposes to which the applicants' personal information may be put, and these undisclosed purposes are not necessary to the Board's duties in the sense of being legally required. Last, the Complainants say the Board cannot rely on s. 32(b) because applicants have not provided valid consent in the prescribed manner and further contend that it cannot rely on s. 32(c) because the personal information is not being disclosed to another public body.

[95] The Board takes the position that consent under s. 32(b) affords a complete answer to this aspect of the complaint and that the consent provided by an applicant should be respected.

[96] I find that s. 32(a) authorizes the Board's use of the information for its hiring and screening process. The evidence establishes that the personal information is being used by the Board for the purpose for which it was obtained and compiled, namely to assist with screening applicants and identifying those applicants who should be short listed for interviews. Where personal information is being used for the purpose for which it was obtained, or for a use consistent with that purpose within the meaning of s. 34, there is no need to obtain consent in the prescribed manner under s. 32(b). From a privacy perspective, it is good practice to obtain written consent whenever feasible, but it is not strictly necessary to do so if s. 32(a) otherwise authorizes the use.

[97] Although it is not necessary to consider s. 32(b), I will do so because the parties' submissions were primarily focused on it. Under s. 32(b), an individual must identify the information and consent, in the prescribed manner, to the use. As I said earlier, I accept that the consent form meets the prescribed requirements. The remaining question is whether applicants are provided with adequate information regarding the uses to which their personal information will be put.

[98] The introductory page of the Assessment confirms that the Board has asked Gallup to assist with its recruiting and hiring process and that Gallup will record and analyze the responses and forward the assessment results to the Board for use as one step in its hiring process. The consent page says that

[48] Para. 82, Complainant's initial submission.

Gallup will process the information provided and may retain this information as part of a permanent database in the United States. Applicants are then asked whether or not they voluntarily "agree" and "consent"[49] to having Gallup perform these activities and to having their data transferred to the United States. On the basis of these pages, I am satisfied that applicants who have completed the Assessment have consented to having their personal information recorded and analyzed by Gallup for the purposes of sending an assessment result reflecting their teaching suitability to the Board for use in its hiring and screening process.

[99] The Complainants suggest that there are a number of undisclosed purposes, including assessing the applicant's teaching and psychological suitability, providing the applicant with a score as a percentile and screening out applicants at the Board's offices. In my view, all of these uses are subsumed within the original purpose for which the personal information was sought and thus form an integral part of the recruitment and hiring process. The screening function is a necessary part of that process as it is evident that the Board cannot hire all of the individuals who apply. I also do not accept the argument that "indefinite storage" is an undisclosed use. Storage of personal information is not a use. Even if storage were a use, the consent form expressly states that Gallup may retain this information as part of a permanent database in the United States.

[100] Similarly, I reject the argument that disclosure under the *USA Patriot Act* would be an undisclosed use. When a person consents to the transfer of his or her personal information to the United States, it necessarily follows that the information will be subject to the laws in force there. The risk of disclosure under foreign legislation does not constitute a "use" for the purposes of s. 32(b). Nor is there any evidence before me that the Board or Gallup intends to voluntarily disclose or use the information under the *USA Patriot Act*. On the contrary, Gallup asserts, certainly, that it would vigorously defend any attempt by United States authorities to access the information in its database under the *USA Patriot Act.*

[101] I agree with the Complainants, however, that use of the personal information in Gallup's validation process is not a disclosed use. The evidence establishes that Gallup asks randomly selected clients to complete an evaluation of 10% of annual new-hire teachers who have completed the Assessment as a means of validating Gallup's process. This does not occur until a client has used the assessment tool for three years. I find that the use of personal information in the validation process is not a use that falls within the scope of the consent because the validation process is not disclosed in the introductory or data consent pages of the Assessment and it is not subsumed under the disclosed purposes.

[49] Gallup's data consent form uses both "agree" and "consent".

[102] The Board acknowledges that consent to the Assessment does not imply consent to a later use of the information for the purpose of validating Gallup's research. If Gallup in the future asks the Board to complete such evaluations, the Board indicates that it intends to seek the written consent of the teachers involved before it discloses the relevant evaluations to Gallup. The Complainants question what the Board will do when teachers refuse to consent to having their personal information used in the validation process. This concern is speculative at this stage, particularly in light of the Board's position. Further, a teacher who refused to consent to the use of her or his personal information in the validation process would have grounds to file a complaint under FIPPA if his or her personal information were used despite the absence of consent.

[103] For the reasons given above, I find that the Board's use of the personal information collected in the Assessment is authorized under s. 32 of FIPPA.

4.0 CONCLUSION

[104] For the reasons given above:

1. Subject to para. 2, below, I find that s. 26(c) of FIPPA authorizes the Board to collect personal information using the Assessment and under s. 58(3)(a) I confirm that the Board has performed its duty under s. 26(c);

2. I find that s. 26(c) does not authorize the Board to collect the social insurance numbers of external applicants and under s. 58(3)(e) I require the Board to stop collecting this personal information from applicants; and

3. I find that the Board has complied with ss. 30, 30.1 and 32 of FIPPA and under s. 58(3)(a) of FIPPA I confirm that the Board has performed its duties under those sections.

[105] I will note here that the Complainants asked that I award compensatory damages, but FIPPA gives me no authority to do that even where that might be appropriate.

June 26, 2007

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia