OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Order F08-03

MINISTRY OF PUBLIC SAFETY & SOLICITOR GENERAL

David Loukidelis, Information and Privacy Commissioner

January 31, 2008

Quicklaw Cite: [2008] B.C.I.P.C.D. No. 6
Document URL: http://www.oipc.bc.ca/orders/OrderF08-03.pdf

Summary: The applicant sought access to *Gaming Control Act* reports from casino operators relating to suspected or actual criminal activity within casinos. The Ministry refused access to any information, citing ss. 15(1)(a) and (l) and s. 21 of FIPPA. The Ministry is not authorized by s. 15 or required by s. 21 to withhold access to the records, but is required under s. 22 to withhold some third-party personal information in them. The Ministry is required to sever that personal information and release the remainder of the records to the applicant within 60 days.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, ss. 15(1), 21(1) and 22; *Gaming Control Regulation*, B.C. Reg. 208/2002.

Authorities Considered: B.C.: Order 02-20, [2002] B.C.I.P.C.D. No. 20; Order 04-07, [2004] B.C.I.P.C.D. No. 7; Order 01-52, [2001] B.C.I.P.C.D. No. 55; Order No. 01-11, [2000] B.C.I.P.C.D. No. 13; Order 03-41, [2003] B.C.I.P.C.D. No. 41; Order 01-01, [2001] B.C.I.P.C.D. No. 1; Order No. 261-1998, [1998] B.C.I.P.C.D. 56; Order 03-02, [2003] B.C.I.P.C.D. No. 2; Order 01-21, [2001] B.C.I.P.C.D. No. 22; Order F05-09, [2005] B.C.I.P.C.D. No. 10; Order No. 116-1996 [1996] B.C.I.P.C.D. No. 43; Order 01-36, [2001] B.C.I.P.C.D. No. 37; Order F07-06, [2007] B.C.I.P.C.D. No. 8; Order 03-04, [2003] B.C.I.P.C.D. No. 4; Order 03-05, [2003] B.C.I.P.C.D. No. 5; Order No. 56-1995, [1995] B.C.I.P.C.D. No. 29; Order 01-51, [2001] B.C.I.P.C.D. No. 54; Order 00-41, [2000] B.C.I.P.C.D. No. 44; Order 03-03, [2003] B.C.I.P.C.D. No. 3; Order F06-21, [2006] B.C.I.P.C.D. No. 40; Order 02-22, [2002] B.C.I.P.C.D No. 22; Order 01-53, [2001] B.C.I.P.C.D. No. 56; Order F05-31, [2005] B.C.I.P.C.D. No. 42; Order 01-12, [2001] B.C.I.P.C.D. No. 13; Order 04-20, [2004] B.C.I.P.C.D. No. 20; Order 02-46, [2002] B.C.I.P.C.D. No. 58. **Alta.:** Order 98-001, [1998] A.I.P.C.P. No. 12. **Ont.:** Order PO-2358, [2004] O.I.P.C. No. 308; Order PO-1983, [2001] O.I.P.C. No. 263; Order PO-2526, [2006] O.I.P.C. No. 199; Order P-1545, [1998] OIPC No. 69; Order PO-2397, [2005] O.I.P.C. No. 77, Order M-1084, [1998] O.I.P.C. No. 59; Order P-820, [1994] O.I.P.C. No. 411; Order P-820; Order P-1511, [1998] O.I.P.C. No. 2.

Cases Considered: *Ternette v. Canada (Solicitor General),* [1991] F.C.J. No. 1168; *Ruby v. Canada (Solicitor General),* [2000] 3 F.C. 589 (CA), varied by [2002], 4 SCR. 3; *Boeing Co. v. Ontario (Ministry of Economic Development and Trade*, [2005] OJ No. 2851 (Div. Ct.); *Fletcher Challenge Canada Ltd. v. British Columbia (Information and Privacy Commissioner),* [1996] B.C.J. No. 505 (SC); *Canadian Broadcasting Corp. v. Northwest Territorie*s, [1999] N.W.T.J. No. 117 (SC); *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, [2006] SCJ. No. 13; *(Minister of Consumer and Commercial Relations) v. Fineberg*, Toronto Doc. 220/95 (Ont. Div. Ct.) leave to appeal refused, [1996] OJ No. 1838 (CA); *Architectural Institute of British Columbia v. Information and Privacy Commissioner for British Columbia,* 2004 BCSC 217.

TABLE OF CONTENTS

1.0 INTRODUCTION 2

2.0 ISSUES 3

3.0 DISCUSSION 4

3.1 Role of the Gaming Policy and Enforcement Branch 4
3.2 Description of Records 7
3.3 Harm to Law Enforcement 8
3.4 Third-Party Business Interests 18
3.5 Third-Party Privacy 25

4.0 CONCLUSION 34

1.0 INTRODUCTION

[1] This inquiry concerns an information access request that a reporter ("applicant") made to the Ministry of Public Safety and Solicitor General ("Ministry") for reports, made under s. 86(2) of the *Gaming Control Act*, about suspected or actual illegal activities in registered gaming establishments and casinos. The Ministry maintains that these reports ("s. 86 reports") are properly withheld in their entirety under ss. 15 and 21 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The applicant disagrees and also questions whether the Ministry has complied with its duty to sever under s. 4(2) of FIPPA.

[2] The Ministry originally denied access to all of the requested records, relying only on s. 15 of FIPPA. The applicant requested a review by this Office and, because mediation was not successful, the matter proceeded to inquiry under Part 5 of FIPPA. At the inquiry stage, but before initial submissions were received, three things worth noting happened.

[3] First, the Ministry told the applicant in December 2005 that it intended also to rely on s. 21 of FIPPA to justify its withholding decision. The reason given was that the release of the records could reasonably harm the business interests of the gaming establishments which authored the reports.

[4] Second, the applicant agreed to revise and limit the scope of the access request. Initially, the applicant's access request was for "records relating to suspected or real offences occurring at registered casino and gaming establishments" in British Columbia—and specifically for all s. 86 reports, from January 1, 1997 forward—which the Ministry estimated would comprise over 2600 records. On March 24, 2006 it was agreed that the scope of the inquiry would be limited to s. 86 reports made by casinos only and any equivalent documentation provided to the Ministry by casinos prior to s. 86 coming into force in August 2002.

[5] Third, in March 2006 when all responsive records had been identified and received by this Office, we notified, under s. 54 of FIPPA, those casino operators whose employees had authored the s. 86 reports and invited them to participate as third parties. The four casino operators that this Office notified were Gateway Casinos Inc. ("Gateway"), Great Canadian Casinos Inc.[1] ("Great Canadian"), 585 Holdings Ltd., Edgewater Casinos Inc. and Treasure Cove Casino.[2] Only Great Canadian and Gateway made submissions in the inquiry. They support the Ministry's decision to withhold the records under s. 21 of FIPPA. Gateway relies in the alternative on s. 22 to say that personal information in the records relating to its customers and employees should not be disclosed. The applicant objects to the s. 22 exception being raised for the first time after he had filed his initial submissions. In the alternative, he objects to reliance on s. 22 to justify a blanket denial of access to all of the s. 86 reports.

2.0 ISSUES

[6] These are the issues raised in this inquiry:

1. Does s. 15 of FIPPA authorize the Ministry to refuse access to all or part of the s. 86 reports?

2. Does s. 21 of FIPPA require the Ministry to refuse access to all or part of the s. 86 reports?

3. Can s. 22 be raised at the late stages of the inquiry process and, if so, does s. 22 of FIPPA require the Ministry to refuse access to all or part of the s. 86 reports?

[7] With respect to ss. 15 and 21, the Ministry bears the burden of proof under s. 57(1) of FIPPA and, under s. 57(3)(a) of FIPPA, the applicant has the burden of proof with respect to s. 22.

---

[1] This party's submission stated that it was from the "Great Canadian Gaming Corporation, its wholly-owned subsidiary Great Canadian Casinos Inc., and Jack O'Clubs Gaming Hall Ltd., a company in which Great Canadian Gaming Corporation holds a controlling interest (collectively, "Great Canadian")"; para. 1, Great Canadian's initial submission.

[2] I refer below to Gateway and Great Canadian collectively as the "Casino Operators".

3.0 DISCUSSION

[8] **3.1 Role of the Gaming Policy and Enforcement Branch**—The Ministry's Gaming Policy and Enforcement Branch ("GPEB") regulates, under the *Gaming Control Act*, all gaming operations, facilities, employees, equipment and activities in British Columbia. A review of that Act reveals that the GPEB oversees the British Columbia Lottery Corporation ("BCLC"), all gaming service providers and gaming workers, the horse racing industry and licensed gaming events. Section 23 of the *Gaming Control Act* specifically provides that the GPEB is "responsible for the overall integrity of gaming and horse racing" and, in furtherance of this responsibility, the GPEB has been given broad investigatory, audit, inspection, licensing, registration, enforcement and compliance powers. Not only must gaming operators be registered under the Act, but all gaming personnel must also be individually registered and are subject to background investigations every five years to ensure their continued suitability and good character. The GPEB general manager has powers to suspend, revoke or cancel registrations and licenses, and may also impose administrative fines (up to $20,000) in appropriate circumstances. For example, under s. 68 of the *Gaming Control Act*, the general manager can refuse to issue or renew the registration of a gaming service provider or gaming worker if there are reasonable grounds for considering the applicant "to be a detriment to the integrity or lawful conduct or management of gaming".

[9] To facilitate the GPEB's compliance and enforcement mandate, the *Gaming Control Act* gives the general manager broad powers to ensure that regulated entities comply with the legislation. For example, s. 71(3) requires a registrant to provide the general manager with reports and information specified by him for the purposes of determining compliance under the *Gaming Control Act*. Section 78 provides for the appointment of inspectors with broad powers under s. 79 to enter and inspect gaming facilities and premises and to require production and permit removal of records or other things for purposes which include "monitoring compliance of licensees, eligible organizations and registrants with [the] Act, the regulations, the rules and the conditions of licences and registration". Section 81 allows the general manager to designate investigators to conduct investigations "for the administration and enforcement" of the Act. Investigation reports must be reported by the general manager to the Attorney General "if the results raise issues that the general manager considers warrant the attention of the Attorney General".

[10] In support of its submissions, the Ministry filed an affidavit sworn by Derek Sturko, the Assistant Deputy Minister and General Manager of GPEB, as well as an affidavit sworn by Larry Vander Graaf, the Director of the GPEB's Investigation Division. In his affidavit, Derek Sturko explains that GPEB's investigative functions are carried out by staff in GPEB's Investigation Division, all of whom are designated as special provincial constables under the *Police Act.* These investigators investigate any alleged contraventions of the *Gaming Control Act* and have authority to issue violation tickets for fines up to $500 for regulatory

offences under s. 97 of the *Gaming Control Act*. These fines could be in addition to any administrative sanctions the general manager imposes for a registrant's failure to comply with the *Gaming Control Act*, the *Gaming Control Regulation*,[3] its registration conditions or any relevant procedures, agreements, policies and orders. Such administrative sanctions or penalties can include written warnings, suspension or cancellation of a service provider's registration, imposition of additional registration conditions or variation of conditions, administrative fines up to $20,000, and the imposition of costs and fees associated with any background investigations carried out by the GPEB. Additionally, and in co-operation with law enforcement agencies—particularly the Royal Canadian Mounted Police Integrated Illegal Gaming Enforcement Team—GPEB investigators assist in the investigation of gaming-related offences under the *Criminal Code*.

[11] Sections 82, 82.1 and 82.3 of the *Gaming Control Act* contain broad search and seizure powers, as well as authority to detain and forfeit gaming supplies in certain circumstances. Section 83 gives the general manager the authority to order that property be frozen if he has reasonable grounds to believe that a licensee, eligible organization, gaming services provider or gaming worker has contravened a requirement of the *Gaming Control Act*, the regulations, rules made under that Act or licence or registration conditions. In addition to these powers, which are aimed at monitoring and ensuring compliance with the *Gaming Control Act*, s. 86 provides as follows:

> 86(1) The lottery corporation must provide to the general manager any information, records or things requested by the general manager that are relevant to an investigation or an investigative audit under the Act.
>
> (2) The lottery corporation and a registrant or licensee must notify the general manager immediately about any conduct, activity or incident occurring in connection with a lottery scheme or horse racing, if that body, registrant or licensee considers that the conduct, activity or incident involves or involved
>
> (a) the commission of an offence under a provision of the *Criminal Code* that is relevant to a lottery scheme or horse racing, or
>
> (b) the commission of an offence under this Act or the regulations.

[12] Any casino that has a contract with the BCLC to provide operational services is a "registrant" for s. 86(2) purposes. Section 86(2) requires registrants like the Casino Operators to report activities described in that section. This duty is reinforced by s. 34 of the *Gaming Control Regulation*, which provides in part that one of the conditions of the registration of a gaming services provider is that it "immediately report to the general manager any conduct or activity at or near a gaming facility that is or may be contrary to the *Criminal Code*, the Act or the regulations".

[3] B.C. Reg. 208/2002.

[13] Derek Sturko deposes that, as general manager, he has issued guidelines to help registrants understand their reporting requirements under s. 86(2).[4] These guidelines identify the types of reportable activities to include any real or suspected:

- Cheating at play
- Theft affecting the integrity of gaming from the casino patrons or employees
- Fraud
- Money laundering
- Loan sharking
- Assault
- Persons barred for known or suspected criminal activity
- Unregistered gaming workers
- Persons suspecting of passing counterfeit currency
- Robbery
- Threats against a gaming employee.

[14] The Ministry has also developed forms for s. 86(2) reporting by service providers. Reports are made on these forms and then sent to both the GPEB's Investigation Division and the BCLC by secure email. All s. 86 reports are investigated by GPEB investigators, as are complaints by third parties about suspected illegal activities in gaming establishments. Reports may be retained and used as "intelligence",[5] which is described in Larry Vander Graaf's affidavit as "any information that identifies an individual, place, time or technique that is involved or suspected to be involved in criminal activity".[6] Reports may also be shared with law enforcement agencies—Derek Sturko estimates that about 55% of reports fall into this category—if it is believed they might assist other investigations. Further, the Ministry says that it does not often lay criminal or regulatory charges as a result of a s. 86 report. It says, however, that s. 86 reports are often grouped together to help investigators identify a technique which criminals are using, as well as the extent of criminal activities.[7]

[15] As the applicant points out in his initial submission,[8] British Columbia's Office of the Auditor General, in its 2005 report *Keeping the Decks Clean: Managing Gaming Integrity Risks in Casinos*,[9] says that "significant consequences exist for government if it fails to adequately ensure gaming integrity in casinos: Unsavoury elements (*e.g.* organized crime and dishonest individuals) may become involved in the industry, posing a threat to patrons, and increasing the level of crime".[10] Section 86(2) appears to be a legislative

[4] Sturko Affidavit, Exhibit A.
[5] Para. 16, Sturko affidavit.
[6] Para. 7, Vander Graaf affidavit.
[7] Paras. 5.06-5.11, initial submission.
[8] At para. 7, initial submission.
[9] Report 5, 2005-2006. http://www.bcauditor.com/PUBS/2005-06/Report5/Casinos.pdf.
[10] Ibid., p. 1.

recognition that gaming establishments may attract "unsavoury elements" and, consistent with the goal of ensuring the integrity of gaming, it is designed to monitor, discourage and combat crime by requiring gaming operators to report any suspected or actual criminal activity. It provides a means by which the gaming industry can be monitored and appropriate steps can be taken where suspected or actual criminal activity takes place.

[16] **3.2 Description of the Records**—The records consist of reports and related records provided to the GPEB and the BCLC by the four Casino Operators on or after April 2002, when the *Gaming Control Act* was given first reading in the Legislative Assembly. Before then, casinos were not required to report suspected illegal activity. The Ministry reports that, since s. 86(2) came into force, it has received approximately 2,400 reports each year and the number is rising.[11]

[17] Because of the nature of the arguments advanced by both the Ministry and the Casino Operators, a detailed description of them is warranted. There are thousands of unnumbered pages of responsive records. They consist of completed s. 86 forms, surveillance reports, emails (internal and with external bodies such as casino operators) and faxes. Typically, the s. 86 forms sent to GPEB contain the name of the casino operator, the date, time and location of the suspected criminal activity, whether the police were called, who made the report and some details about the incident. The type of information in these records ranges from file opening information, to reports on different types of incidents occurring both inside a casino or outside, in the vicinity of a casino.

[18] The types of reported incidents range from removal of barred or self-excluded patrons, removal for refusal to produce identification, altercations between patrons, domestic disputes, attempts by underage or barred patrons to gain access, assaults, threats of harm, attempted theft or theft from patrons or the casino, vehicle damage or vehicle theft, intoxicated patrons, suspected or actual illegal drug use or activity by patrons, staff cashier shortages, damage to casino property (*e.g.,* patron damaging a surveillance camera), armed robbery, use of suspected counterfeit bills, cheating and medical emergencies. Some reports describe bad behaviour by patrons—such as a patron trying to pull the wig off another patron, a patron "mooning" several other patrons, swearing at other patrons or casino staff, aggressive, rude or otherwise inappropriate language or gestures by casino patrons—which results in the patrons being barred from the casino for varying periods. Some reports relate to patrons who leave their children unattended in their vehicles or in hotel lobbies while they attend casinos. Others relate to the activities or conduct of casino staff. Some relate to patrons who express suicidal thoughts.

[19] Some records indicate the file is to remain open pending the results of further inquiries. Others indicate the incident will be recorded for information

[11] Para. 5.08, initial submission; paras. 14-15, Sturko affidavit.

purposes with or without a notation such as "no further action to be taken". Some are marked "concluded". In some cases, the police are called by the casino about an incident, but in others they are not. Many of the individuals who are the focus of a report are identified by name and, in these cases, often some other identifying information is included. Some records contain a good deal of information about an incident. However, the details provided in the majority of them are brief—one or two sentences or less (*e.g.*, a phrase) or one or two brief paragraphs. A relatively small number of them (probably fewer than 200) refer briefly to the results of a videotape review and an even smaller number of them (probably fewer than 50) identify or refer to a camera by a number or similar description. Most often they refer to the observations or actions of surveillance staff or a staff member's description of what she or he saw and did.

[20] Among the records that the Ministry supplied to me for this inquiry, I noted a few reports that pertain to bingo halls. As the request was narrowed to records related to casinos only, I have not included the bingo hall records in my consideration of the issues, as these records are clearly outside the scope of the access request and thus not properly in issue here.

[21] **3.3 Harm to Law Enforcement**—The Ministry relies on s. 15(1)(a) and s. 15(1)(l) of FIPPA, maintaining that disclosure of the disputed records could reasonably be expected to harm a law enforcement matter (its ability to investigate and enforce gaming and *Criminal Code* offences) and could reasonably be expected to harm security and surveillance systems in place in casinos.[12] It further relies on the so-called "mosaic effect" to justify the wholesale withholding the entirety of the responsive records rather than releasing severed versions of them.

[22] Section 15 of FIPPA contains a number of different provisions aimed at protecting law enforcement activities. Section 15(1)(a) and 15(1)(l) incorporate a harms test:

> 15(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to
>
> (a) harm a law enforcement matter; …
>
> (l) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system; ....

[23] Schedule 1 of FIPPA defines "law enforcement" as follows:

> **"law enforcement"** means
>
> (a) policing, including criminal intelligence operations,
>
> (b) investigations that lead or could lead to a penalty or sanction being imposed, or

[12] Paras. 5.15-5.16, initial submission.

> (c) proceedings that lead or could lead to a penalty or sanction being imposed.

[24] As regards s. 15(1)(a), the applicant says it does not apply because the s. 86 reports are not prepared by a law enforcement agency.[13] It adds that even if they are, the Ministry has not shown that any of the harms in s. 15 could reasonably be expected.[14]

[25] Previous orders, such as Order 02-20[15] and Order 04-07,[16] have held that a complaint that initiates an investigation into a possible violation of the law is properly characterized as being a law enforcement matter. Section 86 reports are statutorily required and they trigger investigations by GPEB investigators—who are, as noted above, special constables—that lead or could lead to a penalty or sanction being imposed on a gaming establishment or employee or the laying of criminal charges. I am therefore satisfied that s. 86 reports qualify as "law enforcement" as defined in paragraph (b) of the FIPPA definition.

[26] As for s. 15(1)(l), the Ministry relies on Ontario Order PO 2358[17] for the proposition that a casino's video camera surveillance system is a "system" designed to protect against and detect unlawful acts which would be harmed if details of camera locations and capabilities were disclosed.[18] I accept that a casino's video camera surveillance system which is designed to protect against and detect illegal activities is a "system" within the meaning of s. 15(1)(l) and the evidence establishes to my satisfaction that the details and capabilities of such a system are kept confidential from all but surveillance staff in order to protect against wrongful exploitation of any system weaknesses. Combined with the presence of security officers, camera equipment and surveillance staff, the video camera system enables a casino operator to observe, monitor and record the interior and exterior areas of a gaming facility by both visible and more surreptitious means. This is consistent with GPEB standards and rules which, as one of the Casino Operators points out, requires casinos to:

> … undertake physical and electronic viewing, monitoring and recording of gaming facilities and properties, including gaming activities, facility assets, revenue, customers and employees, through alarm systems, cameras, video and digital camera records, lighting, physical escorts and foot patrols.[19]

[27] The real question, however, is whether the disclosure of some or all of the information in the records creates a reasonable expectation of harm to law enforcement under s. 15(1)(a) or, in the case of s. 15(1)(l), a reasonable

---

[13] Para. 19, initial submission.
[14] Paras. 11-26, reply submission.
[15] [2002] B.C.I.P.C.D. No. 20.
[16] [2004] B.C.I.P.C.D. No. 7.
[17] [2004] O.I.P.C. No. 308, at p. 4.
[18] Para. 5.29, initial submission.
[19] Para. 14, Bolton affidavit, Great Canadian's initial submission.

expectation of harm to casino operator camera surveillance security systems. As I have said many times before, the evidence required to establish that a harms-based exception like those in ss. 15(1)(a) and (l) must be detailed and convincing enough to establish specific circumstances for the contemplated harm that could reasonably be expected to result from disclosure of the withheld records; it must establish a clear and direct connection between the disclosure of the withheld information and the alleged harm. General speculative or subjective evidence will not suffice.

[28] The first harm the Ministry identifies relates only to s. 15(1)(a) and is based on a concern that disclosure of the s. 86 reports would result in future under-reporting of suspected or actual criminal activity because casino operators would fear loss of business and poor public relations as a result of their casinos being connected to illegal behaviour. According to the Ministry, casino operators "are adverse [*sic*] to the public scrutiny that can come from the release to the public of reporting detailing real or suspected activities".[20] This anticipated under-reporting by the casino operators would, the argument goes, in turn result in harm to a law enforcement matter. The Ministry says the logical result of under-reporting will be that the GPEB's ability to investigate *Gaming Control Act* and gaming-related *Criminal Code* contraventions will be compromised because its access to law enforcement intelligence will be reduced and, in turn, fewer cases will be investigated and prosecuted.[21] The Ministry says its fear of under-reporting by casino operators is not merely speculative and, to make this point, it provided some supporting *in camera* evidence. The Ministry also argues that the anticipated under-reporting would be difficult to prove because s. 86(2) is cast in subjective language—"reports are only required when the service provider 'considers' that a real or suspected incident has occurred".[22]

[29] Despite the broad regulatory enforcement powers provided for in the *Gaming Control Act*, which I have described above, the Ministry goes so far as to say that "it would have little or no recourse under the current legislation to force the Third Parties to provide full compliance".[23] This is a rather remarkable proposition since the *Gaming Control Act* gives GPEB staff broad inspection and investigation powers aimed at assessing registrant compliance. For example, inspectors can enter and inspect casinos, can conduct spot checks and can remove records, such as video surveillance tapes, for this purpose. Another example is s. 85, which provides that the "lottery corporation, the general manager or a person authorized by the general manager may place a gaming site under video surveillance to ascertain compliance with this Act, the rules or the regulations". I do not accept that the supposedly "subjective language" in s. 86(2) would make under-reporting difficult to prove. The reporting requirement is clear in its terms and intent and it has been supplemented by the issuance of

[20] Para. 5.23, initial submission.
[21] The Casino Operators expressed these same concerns, but in the context of s. 21 of FIPPA.
[22] Paras. 5.20-5.28, initial submission; paras. 38-45, Sturko affidavit; paras. 16-20, Vander Graaf affidavit.
[23] Para. 5.27, initial submission.

guidelines and educational initiatives to ensure that its scope is fully understood. If GPEB has reason to believe that casino operators are intentionally failing to comply with the spirit and intent of the mandatory reporting requirement, then, as the regulator, it can take the steps necessary to deal with that.

[30] Casino operators would also likely under-report, according to the Ministry, because they would fear for employee safety. Employee safety would be put at risk because the release of the s. 86 reports could allow a criminal or a criminal organization to determine which employee reported his or its activities.[24] While there may be individual circumstances where an employee's safety is a reasonable concern, it would certainly not be so in every case and cannot justify withholding all s. 86 records on this basis. The Ministry did not direct my attention to any specific record where the circumstances could be said to be such that an employee's safety would likely be jeopardized by the release of a particular s. 86 report.

[31] For his part, the applicant points out that the Ministry has acknowledged that there is at present substantial compliance by service providers with the reporting requirement and that this is attributable to factors such as the statute-based obligation to report, an education process that has taught service providers what the law requires of them, the release of guidelines for determining what a reportable incident is and the deterrent effect of administrative penalties and even prosecution.[25] (In one case, a casino operator was fined $15,000 for non-compliance with the s. 86 reporting obligation.[26])

[32] The applicant also says that the arguments advanced by the Ministry are too speculative to meet the harms-based requirements and that any fear of under-reporting

> …can be overcome in an environment where there is not only a legal requirement to report, but where the government has ultimate licensing power over service providers. This is a power that one would hope is exercised to ensure more than bare compliance as a condition of being granted the privilege to operate a casino in the province, earning substantial revenue by facilitating popular gaming activities – activities that are otherwise illegal. The assertion … that the Ministry will have "little or no recourse" to force "full compliance" is unsupported by convincing evidence, and contrary to the logic inherent in the full scope of the Ministry's powers under the Act.[27]

[33] The type of harm the Ministry alleged is similar to the type of harm asserted by what was then the Ministry of Water, Land and Air Protection in

[24] Para. 5.24, initial submission; para. 32, Sturko affidavit.
[25] Para. 13, applicant's reply submission.
[26] Para. 22, Sturko affidavit.
[27] Para. 18, applicant's reply submission.

Order 01-52.[28] As in that case, the Ministry's argument here verges on a claim that, as regards casino operators' s. 86 reporting activities, s. 15(1)(a) provides a class exemption to the right of access to records under FIPPA. The issue in Order 01-52 was whether two conservation groups should be given access to geographic grizzly bear kill location data recorded by the Ministry on the basis of descriptive information provided by hunters. The Ministry, relying on s. 18 of FIPPA, resisted disclosure of this information in part because of concerns that many hunters would refuse to voluntarily provide information to the Ministry and, in the case of compulsory reporting, would "provide inaccurate or overly vague data in the future", which would in turn seriously undermine its harvest reporting system and result in damage to and interference with the conservation of vulnerable wildlife species in the province. I readily held in Order 01-52 that it would be improper for the public body to rely on the argument that, if the disputed records were released, hunters would cease to comply in a proper or meaningful way with the reporting requirements imposed on them by law:

> ¶141 …[I]t is not tenable for the application of the Act to be determined by the possibility that persons given a legal authority - in this case, the legal authority to hunt grizzly bears - will act outside that authority if access to information is granted under the Act [FIPPA]. To accept this…would in my view both subvert the rule of law and the purposes of the Act.…the expectation of harm contemplated in s. 18(b) of the Act is not satisfied because some of those who hold licenses, permits or authorizations to hunt under the *Wildlife Act* may be willing to break the law if they cannot impose disclosure limitations or conditions on the harvest information that the law requires them to provide to the Ministry. The answer to this issue is not to find that the s. 18(b) disclosure exception applies, but rather, if necessary, to grant licenses, permits or hunting authorizations only to those who in some way demonstrate that they will comply with all associated legal requirements.

[34] My conclusions in Order No. 01-52 apply here. The answer is not for me to find that the s. 15 harms-based exception applies because casino operators might willingly break the laws that authorize their activities and regulate them. Risk of harm in this context cannot reasonably be defined by the threat that a regulated industry or any one regulated organization will subvert or ignore mandatory statute-based reporting requirements.

[35] The Ministry also relies on the mosaic effect as the basis for establishing harm under both s. 15(1)(a) and s. 15(1)(l).[29] Turning first to s. 15(1)(a), the Ministry relies on Order 03-41[30] to say that, while disclosure of some of the disputed records might not appear to harm law enforcement, "they should still be

---

[28] [2001] B.C.I.P.C.D. No. 55. Also see the 'chilling' argument made unsuccessfully in Order 01-11, [2000] B.C.I.P.C.D. No. 13.
[29] Paras. 5.33-5.51, initial submission.
[30] [2003] B.C.I.P.C.D. No. 41.

withheld from disclosure as they form part of an overall picture of activities of the casino".[31] This notion is reflected in Larry Vander Graaf's affidavit:

> 10. Often, the Section 86 Reports are not used directly to lay a criminal or regulatory charge. Instead, the reports are akin to puzzle pieces. They can be pieced together by investigators to give them a picture of any larger more organized criminal activity taking place in, and relating to, the casino. In other words, Section 86 Reports are not used in isolation, instead they are often part of a number of similar reports. Reports that can be grouped are more valuable to investigators as these "groupings" of reports help investigators identify the technique that the criminals are using and the extent of criminal operations.
>
> 11. For example, every time a casino receives a counterfeit bill, the identity of the patron should be reported in a Section 86 Report. If through receiving numerous Section 86 reports the Investigators see that a single individual is passing counterfeit bills on a number of occasions, or at a number of different casinos, it becomes clear to them that the patron is directly involving in counterfeiting. Another example is that Section 86 Reports are also used to note incidences of chip passing (transfers of casino chips between individuals). One incident of chip passing does not tell the investigators much, however, when multiple Section 86 Reports reveal that certain patrons are repeatedly involved, they can be identified as likely involved in loan sharking or money laundering.

[36] The Ministry makes the same kind of argument to support the application of s. 15(1)(l). According to the Ministry, release of the s. 86 reports would reveal confidential aspects of casino surveillance and security systems, in turn allowing criminals to acquire more information on how to work around those systems and surveillance investigative techniques. The result would be, the Ministry says, that criminals would have more success in compromising the integrity of or exploiting games, planning or committing criminal acts and facilitating unlawful acts.[32]

[37] The applicant says such a blanket denial of access "flies in the face" of FIPPA's stated s. 2 purposes and the mandatory reporting requirement under the *Gaming Control Act*, a requirement that the applicant says provides the only basis on which the public can monitor the success or failure of efforts to deal with criminal activity in gaming establishments. The applicant argues that there is a significant public interest at stake in access to this information and makes the point that casinos are only given an exemption from being illegal under the *Criminal Code* as a result of the government's role in extensively regulating them. He goes on to say that there is a "clear need for transparency in an industry at risk for infiltration by organized crime" and that the "public is entitled access to the truth, not simply reassuring platitudes from those in control".[33]

---

[31] Para. 5.44, initial submission.
[32] Paras. 5.52-5.55, initial submission.
[33] Paras. 1-2, 13, initial submission.

[38] The applicant also points out that one of the Casino Operators emphasizes on its website that the regulatory requirements are designed to maintain the integrity of the games played in casinos and to ensure industry participants are persons of good character. This Casino Operator also holds itself out as conducting its business with honesty and integrity, consistent with the highest moral, legal and ethical standards, and as complying with all applicable laws and regulations. From the applicant's perspective, the public should have access to specific information about what kinds of actions have been taken at which casinos so the public can form its own conclusions about the accuracy of these kinds of assurances.[34]

[39] In Order 01-01,[35] I described the mosaic effect as the situation where seemingly innocuous information is linked with other already available information to yield information that is not innocuous and, in an information and privacy context, is excepted from disclosure under FIPPA. As I noted in that case, the term is one that is usually encountered in an intelligence and law enforcement context, but it has also been judicially recognized as having application in an information access context, as illustrated in cases such as *Ternette v. Canada (Solicitor General)*[36] and *Ruby v. Canada (Solicitor General)*.[37]

[40] I also said in Order 01-01 that cases in which the mosaic effect applies will be the exception and not the norm. Order 01-01 provides an illustration of such an exception. In that inquiry, the applicant was an anti-abortion activist who sought access to information relating to the number of abortions carried out at a particular health centre over a two-year period and who intended to publish that information if it were disclosed. The public body refused to disclose it, relying on the exceptions in s. 19 and ss. 15(1)(f) and (l) of FIPPA. In doing so, the public body provided detailed and convincing evidence of a reasonable expectation that the release of the requested information could be used to identify individual abortion service providers and that this in turn put the abortion service-providers at risk of harm. In that case, I applied the mosaic effect on the basis of clear and convincing evidence that requested information could be linked, and was intended to be linked, with already available information to yield information that could directly facilitate criminal or otherwise unauthorized behaviour and that was protected under the claimed FIPPA exceptions.

[41] In support of the application of the mosaic effect here, the Ministry relies on Order 03-41, which concerned a media request for access to records relating to incident reports from licensed adult community care facilities. Relying on s. 22(1) of FIPPA (unreasonable invasion of personal privacy), the public body had denied access to some of the requested records. The withheld information was generally described as identifying information about the health and

---

[34] Paras. 9-12, initial submission.
[35] [2001] B.C.I.P.C.D. No. 1, at para. 40.
[36] [1991] F.C.J. No. 1168.
[37] [2000] 3 F.C. 589 (C.A.), varied by [2002], 4 S.C.R. 3.

well-being of individual facility residents. The public body argued that the disclosure of identifying information about residents, workers or others would be an unreasonable invasion of their personal privacy under s. 22 of FIPPA and, further, that disclosure of identifying information about individuals who report and witness incidents would create a reasonable expectation of harm to law enforcement under s. 15.

[42] I ordered the disclosure of a number of the withheld records. Many did not contain identifiable information about anyone and did not require severing. Others identified individuals (not residents), but only in the context of their professional roles in various mental health fields or their positions as government employees, so I ordered them disclosed. With respect to the balance of the records, the public body stressed the risk of re-identification through the mosaic effect, arising from the disclosure of what appeared to be non-personal information which, when combined with information from other available sources, could be used to re-identify the disclosed information.[38] Based on the evidence the public body submitted, I found it reasonable to expect that some persons would be able to identify individuals if the withheld records were disclosed:

> 52. I find it reasonable to expect that residents (or their families or guardians) and employees in these small facilities who have no access to the requested records would nonetheless be able to identify, from information in the requested records, the other residents and employees who were involved in the incidents.
>
> 53. To give some examples, for an incident report relating to the death of one of six residents of a facility, if the name of the facility and the date of the incident were known, as they are from the summary, then it is reasonably likely that some or all of the people living, working or otherwise regularly attending at the facility would be able to connect the detailed information in the incident report with the death of an identifiable person. The same would apply to incident reports about a suicide attempt by a female youth or a specific action or medical condition of a resident.

[43] I was clear, however, that this did not mean "that isolated entries or words in the requested records cannot be disclosed without identifying or re-identifying individuals or that meaningful information cannot be extracted from the requested records for anonymized disclosure to the applicant".[39] The question was whether it was reasonable to sever and withhold the information of concern for the purposes of s. 4(2) of FIPPA.

[44] The Ministry here urges me to consider the ramifications of releasing all of the s. 86 reports together and "what extra information can be gleaned" from them collectively. The Ministry maintains that the information in the records can be repeatedly referenced in other investigations and that over time, patterns can

---

[38] My predecessor referred to this type of re-identification risk in Order No. 261-1998, [1998] B.C.I.P.C.D. No. 56.
[39] Para. 57, Order 03-41.

emerge that shed light on the activities of criminals in gaming establishments. The Ministry also says that it is not possible for it to provide evidence linking each record to a specific law enforcement matter because the significance of the record "may not yet be clear to the Ministry's Investigators".[40] In other words, it is the possibility that a record may at some point in the future have some unexpected value that requires its non-disclosure. That value is its potential significance when linked to a report made at some future time. The obvious response to such a proposition is that if such a linking document is not yet in existence, there is no reasonable expectation of harm.

[45] The Ministry's mosaic effect argument is highly speculative and unconvincing. The law enforcement value relied on is possible, not probable, and rests entirely on its hypothetical connection to information that does not exist yet and may never exist at all. Moreover, there is no suggestion that the withheld information would reveal information that could reasonably be expected to be harmful to law enforcement were it joined with other publicly available information. The mosaic effect is not, and should never be, applied on a speculative basis because that would be an invitation to simply withhold all kinds of information on the basis that someone might somehow use it in negative ways or that there is some possibility of harm. There is also no justification for applying mosaic effect reasoning to withhold information when the mosaic analysis is a desirable investigative tool for the public body that is available to it independent of disclosure of the requested information.

[46] I also note that the Ministry has not provided me with any concrete examples, referring to any of the withheld records, of where the GPEB has actually used s. 86 reports as "puzzle pieces" potentially revealing *techniques* employed by criminals in illegal activities. Nor has the Ministry illustrated, with reference to specific records, how a particular grouping of records has actually revealed potential or actual criminal activity (although I accept that if, for example, a particular individual is repeatedly associated with the passing of counterfeit bills, there is reason to believe that individual may well be involved in criminal activity). In any event, the Ministry has not explained why the type of harm it identifies could not be addressed by, for example, severing relevant information from the records, such as the names and other identifying information of the targets of the reports, as opposed to withholding the records in their entirety.

[47] As noted earlier, the Ministry also relies on the mosaic effect as the basis for applying the s. 15(1)(l) exception. In this respect, it relies in large measure on Ontario Order PO-2358,[41] which concerned a request by a casino patron for access to a videotape of an incident that led to the patron alleging that two casino employees had assaulted and wrongfully detained him. The Ontario Lottery and Gaming Corporation ("OLGC") offered to allow the individual to view the videotape, but the patron wanted his own copy. The patron's appeal was

[40] Para. 5.50, initial submission.
[41] [2005] O.I.P.C. No. 308.

later withdrawn when he received a copy during the course of civil proceedings. He then revived his access request when he was told that his use of the tape was restricted because it had been disclosed to him during the civil litigation document discovery process.

[48] The OLGC ultimately refused to provide a copy of the videotape, relying on s. 14 of Ontario's *Freedom of Information and Protection of Privacy Act*. The OLGC was concerned that disclosure of the tape might reveal the existence and location of cameras, how cameras scanned the floor, the extent of camera coverage (including any gaps) and what the camera was viewing at any time. Among other things, s. 14 of Ontario's *Freedom of Information and Protection of Privacy Act* gives a public body discretion to refuse to disclose a record if disclosure could reasonably be expected to endanger the security of a "system or procedure established for the protection of items, for which protection is reasonably required". In the course of his analysis, Adjudicator Swaigen commented that he had "also considered the possibility that even if disclosure of this tape alone could not reasonably be expected to result in the harms contemplated…viewing [it] together with other videotapes would have this result".[42]

[49] I do not interpret this as meaning that disclosure of more than one videotape *would* result in the harms contemplated. Rather, Adjudicator Swaigen was simply saying that he had taken this possibility into account when making his decision. Ultimately, the Adjudicator was not satisfied that release of the one videotape would enable the viewer to draw accurate inferences about the level and kind of surveillance being carried out in the casino or that disclosure of one videotape would lead to the disclosure of additional videotapes. He also found the evidence relied on by the public body to establish reasonable expectation of harm to be vague and general:

> … [The OLGC does] not specifically point to anything about the level and kind of surveillance at this casino that does not reflect what the public already know about surveillance systems in casinos. Detailed descriptions of the types of surveillance systems in use at casinos, the scope of coverage of cameras, the level of detail cameras can capture, the makes and models of cameras sold for use in casinos, and legislative standards for casino surveillance are posted on the Internet. The OLGC did not identify any specific aspect of the design, operation, or capabilities of the system that would be revealed by viewing the videotape that is not generally known to the public or easily ascertainable.[43]

[50] Similarly, in this inquiry, the Ministry points to no specific record or collection of records which reveals an unknown or not readily ascertainable aspects of the design, operation or capabilities of camera surveillance security systems in use in a casino. I am not satisfied that the evidence provided by the

[42] Pages 6-7, Order PO-2358.
[43] Page 7, Order PO-2358.

Ministry in support of the application of s. 15(1)(l) establishes a reasonable expectation of harm to such a system or that the disclosure of the records could reveal a more comprehensive picture of unknown or not easily ascertainable system details.

[51] My conclusion respecting s. 15(a) and s. 15(1)(l) is only reinforced by my review of the withheld records, which I have already described generally. For the above reasons, I find that the Ministry is not authorized by s. 15 to refuse to disclose the s. 86 reports.

[52] **3.4 Third-Party Business Interests**—Section 21(1) of FIPPA requires public bodies to refuse to disclose information where disclosure would harm third-party business interests as provided in the section, the relevant parts of which read as follows:

> ***Disclosure harmful to business interests of a third party***
>
> 21(1) The head of a public body must refuse to disclose to an applicant information
>
> (a) that would reveal
>
> (i) trade secrets of a third party, or
>
> (ii) commercial, financial, labour relations or scientific or technical information
>
> (b) that is supplied, implicitly or explicitly, in confidence, and
>
> (c) the disclosure of which could reasonably be expected to …
>
> …
>
> (ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied,
>
> (iii) result in undue financial loss or gain to any person or organization….[44]

[53] In Order 03-02,[45] I reviewed at some length the history of third-party business interest exceptions in access to information laws and referred to the Ontario Commission on Freedom of Information and Personal Privacy report, *Public Government for Private People*. I will not repeat what that report said, but it provides a useful context. That report and, more to the point, the many orders considered in Order 03-02 make it clear that the underlying thrust of this type of exception is the protection of the commercially valuable informational assets of

[44] The Ministry cites ss. 21(1)(c)(i) and (ii) in the heading of para. 5.79 where it discusses s. 21(1)(c). However, its arguments actually relate to ss. 21(1)(c)(ii) and (iii) and so I have considered those provisions.

[45] [2003] B.C.I.P.C.D. No. 2.

a third party. More recent court decisions such as *Boeing Co. v. Ontario (Ministry of Economic Development and Trade)*[46] also illustrate this very clearly.

[54] Each of the three criteria established in ss. 21(1)(a), (b) and (c) must be satisfied before this exception applies and I have concluded, for the reasons given below, that the information in the s. 86 reports does not qualify under either s. 21(1)(a) or (c). I have therefore found it unnecessary to consider whether s. 21(1)(b) applies in circumstances like these where the information at issue is required to be produced to a public body by statute and no statutory mention is made of it having any confidential status.

Section 21(1)(a)

[55] The Ministry, supported by the Casino Operators, maintains that disclosing the disputed records would disclose third-party trade secrets, those trade secrets consisting of either information about a casino's surveillance and security systems or other methods by which suspected criminal activities are detected.[47] In the alternative, the Casino Operators variously argue that their security and surveillance systems constitute "commercial", "financial" or "technical" information for s. 21(1)(a)(ii) purposes.[48]

[56] All of these submissions rely on the premise that disclosure of the s. 86 reports would in fact reveal confidential or secret business information about casino surveillance and security systems in use in casinos. Having reviewed those records, I can say that most of these records do not even refer to security or surveillance equipment. Others may refer to the fact that a camera or videotape was involved in the surveillance but, in context, this would not reveal secret or confidential information or a secret or confidential technique, especially in light of the fact that casino operators are required by the regulator to engage in this type of surveillance and security activity and the fact that it is generally known—and I take notice of it—that cameras, videotapes and other similar surveillance techniques are used extensively to monitor all aspects of activities in and around casinos.

[57] The term "trade secret" is defined in Schedule 1 of FIPPA as follows:

> … information, including a formula, pattern, compilation, program, device, product, method, technique or process, that
>
> (a) is used, or may be used, in business or for any commercial advantage,
>
> (b) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use,

[46] [2005] O.J. No. 2851 (Div. Ct.).
[47] Paras. 5.62-5.68, Ministry's initial submission; pp. 3-13, Gateway's initial submission.
[48] Pages 13-15, Gateway's initial submission.

> (c) is the subject of reasonable efforts to prevent it from becoming generally known, and
>
> (d) the disclosure of which would result in harm or improper benefit.

[58] The Ministry, supported by the Casino Operators, makes a variety of arguments—all of which I have considered but will not repeat here–-in support of the idea that casino surveillance and security techniques and other investigative techniques are "trade secrets" which would supposedly be revealed by disclosure of the s. 86 reports. For example, it is argued that the "commercial advantage" derived from such a "technique" is the minimization of cheating and theft and that the "independent economic value" lies in its "potential" benefits (deterrence) and "actual" benefits (catching criminals in the act). It is also said that the surveillance systems are closely guarded secrets and disclosure of information about them would cause the Casino Operators to lose the advantage of secrecy and permit criminals to exploit weaknesses in the systems.[49] The Ministry summarizes its position this way in its initial submission:

> 5.68 …[T]he Ministry submits that the s. 86 reports contain trade secrets because they reveal information about the methods or techniques by which casinos detect and investigate suspicious activity, and about the capabilities of a casino's surveillance system. This information is protected from the knowledge of the general public and all the staff of the casino (save the surveillance staff) as knowledge of these details can be used to facilitate criminal activity through which a casino loses money.

[59] It is not at all certain what secret methods or techniques are being referred to here. It cannot be a secret that casino operators employ security personnel who physically observe patrons or casino employees within the casino.[50] Nor can it be a secret that casinos use cameras, digital and video surveillance equipment—hidden or not hidden—to monitor goings-on. Surely it is no secret that casino surveillance staff may view what is going on from hidden or closed viewing rooms. It would come as no surprise that surveillance cameras have pan, tilt and zoom capabilities. There are no surprises here, not least because the law requires casino operators to use such techniques and specifically directs that they be carried out in certain areas of the casino in furtherance of the legislative goal of ensuring gaming industry integrity. I am not in the least convinced that the type of information at issue can reasonably be construed as a casino operator's "trade secret". I am reinforced in this by my review of the records, which reveals they do not contain information that could reasonably be construed as a secret method or technique of the sort embraced by FIPPA's definition of trade secret.

[60] Further, while I accept that the details of a casino's surveillance operations and capabilities are the subject of reasonable efforts to prevent them from being generally known, I am also not persuaded that any secret details are actually

---

[49] Paras. 5.61-5.68, Ministry's initial submission; pp. 3-13, Gateway's initial submission.
[50] Indeed the Ministry admits as much at para. 5.63 of its initial submission.

contained in the s. 86 reports. I also question whether such information in the s. 86 reports derives any independent economic value in the sense intended by the FIPPA definition, especially in light of the fact that all casino operators are required by law to establish and maintain comprehensive security and surveillance systems.[51]

Commercial, financial or technical information

[61] Relying on such orders as Order F05-09,[52] Order No. 116-1996[53] and Order 01-36,[54] the Casino Operators also contend that information about the number and type of detected illegal transactions and how those transactions were detected through surveillance and security measures constitutes their "commercial" information for s. 21(1)(a)(ii) purposes.[55] One of the Casino Operators describes it this way:

> 44 The Reports include information of a commercial nature because they contain information which describes the sale, purchase and exchange of goods and services such as chips, tokens and money at the gaming facilities. Information can also be "commercial" if it includes methods a third party proposes to use to provide goods and services (Order F05-09). In the case of the Reports, the information contained therein demonstrates the methods used … to supply gaming services, and in particular surveillance and security services, to the BCLC under the COSAs. We submit that both of these meet the test for "commercial information".[56]

[62] The meaning of "commercial" information for s. 21 FIPPA purposes was recently considered in Order F07-06.[57] In that case, it was noted that previous orders have found that such information

> [20] …relates to commerce or the buying and selling of goods and services, including information about: offers of products and services the entity proposes to sell or perform; the entity's experiences in commercial activities where this information has commercial value; terms and conditions for providing services and products; lists of suppliers or subcontractors compiled for use in the entity's commercial activities or enterprises; methods an entity proposes to use to supply goods and services; and the number of hours an entity proposes to take to complete contracted work or tasks.

[63] The fact that the information at issue may have actual or potential commercial value is not the test. Rather, the information itself must be

---

[51] Order 01-21, [2001] B.C.I.P.C.D. No. 22, at paras. 34-35.
[52] [2005] B.C.I.P.C.D. No. 10, at para. 18.
[53] [1996] B.C.I.P.C.D. No. 43.
[54] [2001] B.C.I.P.C.D. No. 37.
[55] Paras. 13-15, Gateway's initial submission; paras. 42-45, Great Canadian's initial submission.
[56] para. 44, Great Canadian's initial submission.
[57] [2007] B.C.I.P.C.D. No. 8.

associated with the buying, selling or exchange of the entity's goods or services. An example would be a price list or a list of suppliers or customers. Another example is a third-party contractor's proposed and actual fees and percentage commission rates and descriptions of the services it agreed to provide to a public body, as I found in Order 03-04.[58] The names and addresses of commercial entities such as gaming establishments would not normally qualify as commercial information.[59]

[64] I find that the information actually contained in the s. 86 reports is not properly characterized as commercial information for the purposes of s. 21. It is not business information that is associated in a sense contemplated by s. 21 with the buying, selling or exchange of a casino's goods or services. The information at issue has no "commercial" value to casino operator "competitors"—the reports are only generated because they are legally required. Their intended value lies in what the reports reveal to the regulator about the integrity of casino operations and also the use to which the information they contain can be put by the regulator and law enforcement personnel to monitor and enforce compliance with the *Gaming Control Act,* impose administrative and regulatory sanctions and prosecute criminal offences.

[65] One of the Casino Operators also claims that the withheld records disclose "financial" information because "they reveal the use of money in the casino during gambling activities…and the loss of money…due to criminal activity and activity contrary to the *Gaming Control Act*".[60] I do not accept that, even if some of the withheld records may describe (for example) money transactions, the discovery of counterfeit money or thefts taking place within a casino, such information is "financial" information for s. 21(1)(a) purposes. In the context of FIPPA, examples of financial information would include such things as cost accounting methods, pricing policies, profit and loss data, overhead and operating costs, amount of insurance coverage obtained, dollar amount of estimated damage to third party premises caused by fire.[61] It is not suggested—and nor does review of the records support—that the withheld records contain financial data, such as a casino operation's surveillance or security costs.

[66] The Casino Operators also argue that the s. 86 reports contain "technical" information because they relate "to the civilian security craft or profession and security techniques", which is information "of" or "about" the Casino Operator because it "relates to illegal or suspected illegal activities occurring on casino property relating to its gaming services" which is the "sole product of

---

[58] [2003] B.C.I.P.C.D. No. 4.
[59] See Ontario Order PO 1983, [2001] O.I.P.C. No. 263, at para. 86.
[60] Page 15, Gateway's initial submission.
[61] See Ontario Order PO-1983, at paras. 79, 93, 100, and Order PO-2526, [2006] O.I.P.C No. 199, citing Order PO-2010).

observations made by" casino employees and casino surveillance systems. One of the Casino Operators argues it this way:

> …[T]he s. 86 reports disclose information that relates to the civilian security craft or profession and security techniques. Police work is a profession. The civilian equivalent of police work is security and is a craft or profession as it involves training in the observation, investigation, detection and prevention of illegal activities. Some security professionals have been through the police officer training program. Security staff…attend the Gaming Officer Security Course at the Justice Institute to receive certification as Gaming Security Officers. Aspects of the security techniques can be inferred from information in the s. 86 reports as the information is gathered through the use of these techniques.[62]

[67] As was the case in Order F07-06,[63] this does not establish that the type of information in s. 86 reports reflects an organized field of knowledge falling under the general categories of applied sciences or mechanical arts or that the withheld information was prepared by a professional in a recognized related specialty that relates to the observation and testing of certain hypothesis or conclusions. I therefore find that the s. 86 reports do not reveal "technical" information for s. 21(1)(a)(ii) purposes.

Section 21(1)(c)

[68] Having concluded that the information in the s. 86 reports does not reveal trade secrets or commercial, financial or technical information, it is not necessary for me to go further and consider whether the remaining elements in ss. 21(1)(b) and (c) are satisfied. I also find the submissions in support of the application of the s. 21(1)(c) criteria are not persuasive, however, and will give my reasons for this.[64]

[69] The Ministry and Casino Operators rely on ss. 21(c)(ii) and (iii).[65] For reasons that largely duplicate those advanced in support of the law enforcement exemption, they argue that there is a reasonable expectation that disclosure of the s. 86 reports will result in similar information no longer being supplied to the Ministry by casino operators. Despite the fact that s. 86 statutorily compels casino operators to report suspected activity, the Ministry contends that it is reasonable to expect that disclosure of the disputed records will not only result in a decrease in the number of reports received, but also that the quality of the reports will suffer (this is the 'under-reporting' concern I referred to earlier). In this respect, the Ministry asks me to reconsider the approach taken in Order 03-05[66] and similar orders, such as Order 01-51,[67] where I pointed out

---

[62] Page 15, Gateway's initial submission.
[63] At para. 29.
[64] As noted above, I need not deal here with s. 21(1)(b).
[65] Paras. 5.79-5.86, Ministry's initial submission; pp. 22-33, Gateway's initial submission; paras. 51-55, Great Canadian's initial submission.
[66] [2003] B.C.I.P.C.D. No. 5.

that, in the case of *Fletcher Challenge Canada Ltd. v. British Columbia (Information and Privacy Commissioner)*,[68] the Court upheld the determination by Commissioner Flaherty, in Order No. 56-1995,[69] that s. 21(1)(c) is not engaged in circumstances where the information is or could be required to be supplied by law.[70] I see no reason to deviate from the approach taken in these orders and reflected in *Fletcher Challenge*.

[70] Turning next to s. 21(1)(c)(iii), in previous orders, such as Order 00-41,[71] and Order 03-03[72]—and following Vertes J.'s decision in *Canadian Broadcasting Corp. v. Northwest Territories*[73]—I have interpreted "undue" to mean financial loss or gain that is unfair, improper, inappropriate or excessive. Again, the evidence offered in support of loss or gain must be clear and cogent, in the manner discussed above. In essence, the Ministry claims that disclosure of any aspect of the s. 86 reports would cause undue financial loss to casino operators because it would allow criminals to be more successful in their illegal activities. The evidence on this is anything but convincing—it is, in fact, global and speculative. The Casino Operators also foresee that their losses due to the use of counterfeit money, theft and other criminal activities "would be expected to increase" and with increased crime would come increased expenditures on security and surveillance. It is further speculated, among other things, that disclosure of the s. 86 reports could "reasonably be expected to result in undue financial loss…because of financial loss from…revenue from lost customers, loss from perception of increased risk by investors, and lost revenue from employee turnover".[74] In addition, it is argued there will be undue loss of casino goodwill due to a loss of reputation, occasioned by inaccurate references about the type and amount of criminal activities taking place on casino premises.[75] Again, I am not at all persuaded on any of the points made, especially in light of my review of the records and the largely speculative nature of the evidence.

[71] Returning to my earlier description of some of the records, it is hard to see (for example) how criminal activity in casinos would escalate or criminals would benefit financially as the result of disclosure of information about an assault of one patron by another, information about the barring of a patron, information about the removal of a barred patron from a casino, information about the circumstances of a medical emergency, information about the mere discovery of counterfeit bills or reports of abusive, threatening, aggressive or inappropriate conduct by casino patrons. In any event, as I have said, I find the type of evidence adduced in support of s. 21(1)(iii) to be global and highly speculative, certainly too speculative to meet the requirements of FIPPA.

---

[67] [2001] B.C.I.P.C.D. No. 54.
[68] [1996] B.C.J. No. 505 (SC).
[69] [1995] B.C.I.P.C.D. No. 29.
[70] Paras. 5.81-5.82, initial submission.
[71] [2000] B.C.I.P.C.D. No. 44, at para. 36.
[72] [2003] B.C.I.P.C.D. No. 3, at para. 42.
[73] [1999] N.W.T.J. No. 117 (SC).
[74] Page 27, Gateway's initial submission; paras. 35-38, Great Canadian's initial submission.
[75] Pages 27-29, Gateway's initial submission.

[72] For the above reasons, I find that s. 21(1) does not require the Ministry to refuse to disclose the s. 86 reports.

[73] **3.5 Third-Party Privacy**—The Ministry did not apply s. 22 as a basis for withholding information in the records and it was not identified as an issue in the Portfolio Officer's Amended Fact Report for the inquiry or the Notice of Inquiry. My review of the records reveals that the majority of the s. 86 reports contain some personal information. In his initial submissions, the applicant observed that the Ministry had not referred to s. 22 in its initial submissions and so he presumed the records did not raise any privacy concerns. In his reply, the applicant objects to s. 22 being raised during the inquiry and feels that this bears all the indicia of "grasping at straws" to keep the s. 86 reports from the public. The applicant goes on to say that if, despite his objections, s. 22 is considered, it should not form the basis for the total denial of access to all of the information in the s. 86 reports.

[74] In reply, the Ministry says the applicant's assumption that there were no privacy concerns was "incorrect" and explained as follows:

> …As a result of the Ministry's decision that [it was] required by s. 21 and 15 to withhold the records, no consideration of the records in terms of s. 22 was made. In fact, there is a great deal of personal information contained in the s. 86 reports, and, if the Commissioner does order a release of the records at issue, the OIPC has acknowledged in a letter dated February 28, 2006 (attached) that the record will have to be examined for s. 22 severing.

[75] It is true that the February 28 letter from my Office said that the records would not be ordered released without first considering the application of s. 22 of FIPPA. The letter went on to say that, if the Ministry wished to add s. 22 to the inquiry, it would be necessary for it to issue a new decision letter to the applicant. The Ministry did not do so and I regret to say that the letter from my Office was not helpful. To be clear, where (as here) a public body believes a mandatory exception such as s. 22 applies to information in records responsive to an access request, that exception ought to be relied on in the public body's initial response to an applicant or, at the very least, as soon as it subsequently becomes aware that s. 22 should be applied. It is not appropriate to refrain from doing so only because other exceptions to the right of access are being relied on. As Adjudicator Austin-Olsen explained in Order F06-21:[76]

> [15] If a matter has already proceeded to the inquiry stage, and the public body determines that another section of FIPPA applies to the records in dispute, the proper course of action is for the public body to contact the Registrar of Inquiries and advise that it wishes to raise a new issue in the inquiry. However, whether or not a public body, or any party, will be permitted to do so will depend upon the particular circumstances.

[76] 2006] B.C.I.P.C.D. No. 40.

[76] As I indicated at the outset, one of the Casino Operators, Gateway, raised the s. 22 issue in its initial submission. It relied on the Supreme Court of Canada's decision in *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*[77] for the proposition that a participant who is neither a public body nor an individual can independently raise the s. 22 third-party personal information exception.[78] I need not decide whether *Heinz*—which involved different legislative access to information scheme, language and circumstances—supports this proposition because of my conclusions, which I will now explain, about the mandatory nature of s. 22.

[77] Supported by the Ontario Divisional Court in *Ontario (Minister of Consumer and Commercial Relations) v. Fineberg*,[79] a number of Ontario orders have held that the Ontario Information and Privacy Commissioner has the power to control the process by which an inquiry is undertaken, including the authority to limit the time during which a public body can raise new discretionary exceptions.[80] The point has been made in these and other orders that claiming a discretionary exception promptly is necessary to ensure the integrity of the commissioner's process, such as to facilitate effective mediation and to ensure fairness. With respect to the late application of discretionary exceptions, a variety of factors is considered when deciding whether or not to permit a public body to raise them during the inquiry.

[78] Section 22, however, is a mandatory exception to the right of access under FIPPA. Under s. 22, a public body "must" refuse to disclose any personal information in circumstances where the disclosure would be an unreasonable invasion of personal privacy. As regards mandatory exceptions, and consistent with the approach I took in Order 02-22,[81] other jurisdictions have held that, even if raised for the first time during the exchange of submissions, mandatory exceptions must be considered by the adjudicator.[82]

[79] Due to its mandatory nature, and taking into account all of the circumstances, I find it both necessary and appropriate to consider the s. 22 exception as it relates to the s. 86 reports regardless of which or whether a party raised it.[83] Even where s. 22 is not raised in an inquiry, I consider myself obliged to put my mind to its application where, as here, on my review of the records it is apparent s. 22 applies to some information in them. This is consistent with steps

---

[77] [2006] S.C.J. No. 13.
[78] Page 31, Gateway's initial submission.
[79] Toronto Doc. 220/95 (Ont. Div. Ct.), leave to appeal refused, [1996] O.J. No. 1838 (C.A.).
[80] See, for example, Ontario Order P-1545, [1998] OIPC No. 69, Order PO-2397, [2005] O.I.P.C. No. 77, Order M-1084, [1998] O.I.P.C. No. 59 (at p. 10), and Order P-820, [1994] O.I.P.C. No. 411 (at pp. 2-3).
[81] [2002] B.C.I.P.C.D No. 22.
[82] See, for example, Ontario Order P-1545 (at para. 14), Order P-820 (at p. 3), Order P-1511, [1998] O.I.P.C. No. 2 (at p. 2), and Alberta Order 98-001, [1998] A.I.P.C.P. No. 12 (at p. 10).
[83] In reaching this conclusion, I am not applying *Heinz Canada*, above, which dealt with the very different wording of federal legislation.

I have taken in such orders as Order 01-22,[84] where I applied s. 22 to some personal information that the public body had released. I do not consider this to be unfair to any of the parties to the inquiry because the applicant, the Ministry and the other Casino Operator all had the opportunity to make submissions on the application of s. 22 in their reply submissions and both the applicant and the Ministry did so.

Application of s. 22 to the s. 86 reports

[80] I do not have the benefit of any specific s. 22 severing by the Ministry. Therefore, at this point, I can only consider the application of s. 22 to the information in the records in a general way, as a means of providing the Ministry with guidance as to what severing should occur before the remainder of the requested information is released to the applicant.

[81] The proper approach to the application of s. 22 of FIPPA to information in records that are the subject of an access request has been discussed in previous orders, such as Order 01-53.[85] The first step is to determine whether the withheld information is personal information and whether it is personal information of a third party (as opposed to the applicant's own personal information). In this case, the applicant is not seeking access to his own personal information and so the only question is whether the records contain "personal information", which FIPPA defines to mean "recorded information about an identifiable individual other than contact information". "Contact information" is in turn defined in Schedule 1 of FIPPA to mean:

> … information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

[82] As Adjudicator Francis pointed out in Order F05-31,[86] the purpose of this exclusion is to clarify that information relating to the ability to communicate with a person at that person's workplace, in a business capacity, is not personal information and that, accordingly, public bodies need not have s. 22 concerns regarding disclosure of such information when it is sought. Similarly, public bodies need not have s. 22 or Part 3 concerns with respect to publication of this information (for example, in an employee directory or on employee business cards). Whether information will be considered "contact information" will depend on the context in which the information is sought or disclosed. The context here is one where the applicant is not seeking access to the name, address or telephone number of an identifiable individual in any business capacity and so this type of information, where found in the records, is not "contact information" for FIPPA "personal information" definition purposes.

---

[84] [2001] B.C.I.P.C.D. No. 23 (at para. 81).
[85] [2001] B.C.I.P.C.D. No. 56.
[86] [2005] B.C.I.P.C.D. No. 42, at para. 26.

[83] At the outset, I do not accept that disclosure of the names of casino or public body employees would give rise to an unreasonable invasion of their personal privacy where they are acting in a professional or employment capacity. Some examples of this type of personal information include the names and email addresses of GPEB employees and casino employees in email exchanges relating to the s. 86 reports; the names of police officers attending at a casino in response to a particular incident; and the names of casino employees who author s. 86 reports. I have many times before found that the release of the names of employees acting in an employment or professional capacity does not amount to an unreasonable invasion of privacy under s. 22.[87] While the context in these orders was with respect to public body employees, I see no principled reason why this general proposition should not apply equally to the casino employees acting in such capacity.

[84] While an employee's name is personal information, where it appears in the context of the proper performance of her or his employment duties and functions, all it reveals is what the employee did as part of those duties and functions on behalf of the employer. In some jurisdictions, such as Ontario, this type of information has been held not to fall within the personal information definition on the basis that it is not information "about" the identifiable individual. In Order PO-1885,[88] for example, the adjudicator observed as follows:

> [10] …Previous decisions of this office have drawn a distinction between an individual's personal, and professional or official government capacity, and found that in some circumstances, information associated with a person in his or her professional or official government capacity will not be considered to be "about the individual" within the meaning of the section 2(1) definition of "personal information" (Orders P-257, P-427, P-1412, P-1621). Thus, for instance, where information may be described as being related to the employment or professional responsibilities of individuals, such information is not personal in nature, even where the individuals are identifiable (Reconsideration Order R-980015).

[85] Similar thinking can be seen in *Dagg v. Canada (Minister of Finance)*,[89] where the Supreme Court of Canada was considering a provision in the federal *Privacy Act* that exempted from its personal information definition information like that described in s. 22(4)(e) of FIPPA. In dissent, La Forest J., with whom the majority agreed on this point, said that information relating to a public body employee's position is not personal information "even though it may incidentally reveal something about named persons", with this being in distinction to what was described as "information relating primarily to individuals themselves or to the manner in which they choose to carry out the tasks assigned to them".[90]

---

[87] See, for example, Order 03-21, [2003] B.C.I.P.C.D. No. 21; Order 01-15, [2001] B.C.I.P.C.D. No. 16; Order 01-22, [2001] B.C.I.P.C.D. No. 23, at paragraph 82; Order 01-53, Order 00-17.
[88] [2001] O.I.P.C. No. 59.
[89] [1997] 2 S.C.R. 403.
[90] Para. 94.

[86] More recently, in *Canada (Information Commissioner) v. Canada (Canadian Transportation Accident Investigation and Safety Board)*,[91] the Federal Court of Appeal found that the recordings or transcripts of air traffic control communications recorded by NAV CANADA and under control of the Transportation Safety Board did not contain personal information "about" the NAV CANADA employees (who are not officers or employees of a government institution) whose words were recorded or transcribed:

> [54] The information contained in the records at issue is of a professional and non-personal nature. The information may have the effect of permitting or leading to the identification of a person. It may assist in a determination as to how he or she has performed his or her task in a given situation. But the information does not thereby qualify as personal information. It is not about an individual, considering that it does not match the concept of "privacy" and the values that concept is meant to protect. It is non-personal information transmitted by an individual in job-related circumstances.

[87] The idea that information of this kind is not personal in nature, even where the individuals are identifiable, is reflected in other FIPPA provisions, such as the definition of "contact information" and s. 22(4)(e), which presumes that the disclosure of information about a public body employee's "position, functions or remuneration as" an employee will not constitute an unreasonable invasion of personal privacy. I need not adopt this approach here, which is taken in the Ontario orders and which would exclude this information from the FIPPA definition because it is not information "about" the individuals involved. The common thread is that, regardless of whether the information is characterized as not being "about" an identifiable individual or as personal information that lacks a distinctly personal dimension, release of this information would not constitute an unreasonable invasion of personal privacy.

[88] As for the remainder of the personal information in the s. 86 reports, Gateway raised s. 22 in order to "ensure that the identification of its employees' and customers' names, birthdates, addresses … licence plate numbers" and similar personal information contained in the s. 86 reports is not disclosed, should I conclude that ss. 15 and 21 of FIPPA do not apply to them.

[89] Returning to the proper approach to applying s. 22, a review of s. 22(4) reveals that none of the categories listed there has relevance to the remaining personal information. Turning next to consideration of whether s. 22(3) applies to it, Gateway relies on the presumptions set out in s. 22(3)(b) and (d), which read as follows:

> 22(3) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if …
>
> (b) the personal information was compiled and is identifiable as part of an investigation into a possible violation of law,

[91] 2006 FCA 157, leave to appeal denied, [2006] S.C.C.A. No. 259.

> except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation …
>
> (d) the personal information relates to employment, occupational or educational history.

[90] I have in many previous orders considered what "possible violation of the law" means for s. 22(3)(b) purposes. For example, in Order 01-12,[92] I held that gaming licence conditions set by the former British Columbia Gaming Commission under delegated authority were, due to the governing legislative scheme at the time, a "law". Accordingly, a field review report generated by the Gaming Commission with respect to whether a particular establishment was operating in compliance with those licence conditions was found to come under s. 22(3)(b):

> 16. Does the phrase "a possible violation of law" in s. 22(3)(b) include a violation of the BCGC Conditions or any statutory provision associated with them or underpinning them? My predecessor concluded, for the purposes of s. 15, that the term "law" extends to matter that may be criminal, quasi-criminal, regulatory or disciplinary in nature (in the last case, where there is a statutory underpinning for the disciplinary process). I have agreed, for example, that disciplinary proceedings instituted by self-regulating professions under statutory authority quality as "law" enforcement proceedings for the purposes of s. 15(1) … In Order 00-18, I held that the process invoked by the Superintendent of Motor Vehicles, under the *Motor Vehicle Act*, to determine whether someone is fit to drive qualifies as "law" enforcement within the meaning of s. 15(1).
>
> 17. Although I do not foreclose the possibility that there may be other kinds of "law" for the purposes of the Act, I consider that "law" refers to (1) a statute or regulation enacted by, or under the statutory authority of, the Legislature, Parliament or another legislature, (2) where a penalty or sanction could be imposed for violation of that law. The term "law" includes local government bylaws, which are enacted under statutory authority delegated by the *Local Government Act*. I also consider that the definition of "regulation" in s. 1 of the *Interpretation Act* offers guidance in identifying things that may – where a penalty or sanction could be imposed for their violation – properly be considered a "law" for the purposes of the Act….

[91] It is clear to me that the s. 86 reports themselves were compiled and are identifiable as part of an investigation into a possible violation of the law. With a very few exceptions (*e.g.*, the reporting of a patron health emergency), the very subject matter of the withheld reports is suspected or actual criminal activity taking place in casinos which will form the focus of some investigation by the Ministry and, in some cases, the police as well. Personal information in the s. 86 reports – such as the names, addresses, driver's licence numbers, vehicle licence plate numbers, telephone numbers, etc. – of the targets of the report (be they a patron or a casino employee), as well as complainants or witnesses to

[92] [2001] B.C.I.P.C.D. No. 13.

an incident, is also compiled and identifiable as part of such an investigation. It is as clear that, in the circumstances here, disclosure of this third-party personal information is not required in order to prosecute the violation or continue an investigation. I am therefore satisfied that the s. 22(3)(b) presumption against disclosure applies to the personal information of the type I have just described.

[92] As for s. 22(3)(d), I find this presumption would also apply to the name and any other identifying information of a casino employee who is the target of a s. 86 report. As was noted in Order 02-56,[93] upheld in *Architectural Institute of British Columbia v. Information and Privacy Commissioner for British Columbia*,[94] s. 22(3)(d) includes information about a person's work history, leave transactions, disciplinary action taken, reasons for leaving a job and comments about an individual's workplace actions or behaviour in the context of a workplace complaint or discipline investigation. A s. 86 report that focuses on an employee's workplace behaviour is information about the person's work history which may be used for disciplinary purposes and which may even result in criminal charges being laid.

[93] Having determined that disclosure of third-party personal information in the s. 86 reports is presumed to constitute an unreasonable invasion of personal privacy under s. 22(3)(b) and also, in some cases, s. 22(3)(d), the next step is to consider all relevant circumstances, including those specifically enumerated in s. 22(2). As I said in Order 01-53, the relevant circumstances may or may not rebut any presumed unreasonable invasion of personal privacy under s. 22(3) or lead to the conclusion that disclosure would not otherwise cause an unreasonable invasion of personal privacy.

[94] Gateway points to two of the relevant circumstances enumerated in s. 22(2), namely s. 22(2)(e) (the third party will be exposed unfairly to financial or other harm) and s. 22(2)(h) (the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant). Regarding the latter, Gateway argues in part as follows:

> Disclosure of this information may unfairly damage the reputation of any person referred to in the s. 86 reports as both real and suspected activity is included. Individuals identified [as] being involved in suspected criminal activity and activity contrary to the *Criminal Code* would have their reputation unfairly damaged. Although subsequent investigation and the evidence collected provides that the suspicions outlined in the s. 86 report were unwarranted, as their names were disclosed in the s. 86 [reports] the impression left would be that those persons listed actually committed the alleged act.[95]

[93] [2002] B.C.I.P.C.D No. 58, at para. 71.
[94] 2004 BCSC 217.
[95] Page 31, Gateway's initial submission.

[95] The applicant responds, in part, that casino employees know that information is gathered about them for a variety of reasons, including review of their work performance. He points out that, on a website of one of the casino operators, it is said that casino employees are required to agree that they understand video footage obtained through video surveillance may be used for reasons that include monitoring performance and as the basis of disciplinary action. The applicant goes on to argue that it is "disingenuous" for Gateway "to maintain that denial of information referring to employees' conduct in the course of their duties needs to be kept from others, when they have gone to such lengths to ensure that this information is accessible and usable".[96]

[96] To the extent that the personal information is that of a target (or a person implicated with the target), I agree with Gateway that s. 22(2)(h) is a relevant circumstance. These individuals may never even know that they have been identified as being associated with or suspected of criminal activity. In light of the context in which the targeted individual has been identified, the release of his or her personal information could, in my view, unfairly damage that individual's reputation. This relevant circumstance only reinforces the s. 22(3)(b) presumption against disclosure of the personal information of s. 86 report targets. Further, while casino employees are made aware that video surveillance information can be used against them for disciplinary purposes, this alone cannot be treated as a "waiver" of their privacy interests where they are the target of a s. 86 report and it certainly does not overcome the s. 22(3)(d) presumption of unreasonable invasion of personal privacy.

[97] As regards the claim that third parties (for example, casino employees) may be unfairly exposed to harm if their personal information is disclosed, the applicant argues that the Ministry did not raise any privacy issues that suggest a concern for the welfare of individual employees and that, if Gateway's s. 22 concerns in this regard "were real, they would have been advanced earlier, and in a more focused manner, dealing with the protection of specific individuals in specific circumstances."[97] Taking all of the *in camera* and open evidence into consideration, including the records themselves, I am not convinced there is a case for the application of s. 22(2)(e) to the personal information of either casino employees or patrons, regardless of whether they are named as targets, employees, witnesses or complainants.

[98] Last, the applicant argues there is a strong public interest in releasing the personal information, regardless of whether it is personal information of a patron or employee and regardless of whether the individual is a target or witness:

> 49. As targets, there is a strong public interest in knowing who is being investigated, whether they are targeted fairly, or repeatedly, and what is the

[96] Paras. 45-46, applicant's reply submission.
[97] Reply submission, para. 23.

> outcome of the investigation. Knowing who is involved is essential to tracking their cases, and ensuring that all are treated equally. Those who are targeted may well want and deserve to get access to the s. 86 reports about them, to ensure they are fairly treated.
>
> 50. As witnesses, their identities are likely already known to the suspects, and especially so if the investigation has resulted in has resulted in charges being laid and the required disclosure to the defence has taken place. We have no interest in discovering the identities of confidential informants, unless their identities are revealed in the normal course.[98]

[99] I do not find the applicant's general public interest arguments compelling. The presumptions in ss. 22(3)(b) and (d) speak to a public interest in generally withholding this type of information. The applicant does not have a personal interest in the records he seeks. It is not suggested, for example, that he believes himself to have been unfairly targeted. In relation to the identities of witnesses, it is pure speculation to say they are "likely already known to the suspects".

[100] For the sake of completeness, I acknowledge that Gateway maintained that a summary of any withheld personal information should not be supplied under s. 22(5) as it "cannot be prepared without disclosing the identity of a third party who supplied" it. Section 22(5) has no relevance here. It only applies to an applicant's personal information and then only in circumstances where it has been supplied in confidence.

[101] In summary, the s. 22 guidelines that I find are to govern the Ministry's severing of third-party personal information from the s. 86 reports are as follows:

> 1. The names, position titles and other work-related identifying information (such as a business telephone number or email) of public body and casino employees must be disclosed to the applicant where the context is one where they are acting in a professional or employment capacity. Some examples include: the names and email addresses of GPEB employees and casino employees in email exchanges relating to s. 86 reports; the names of police officers attending at a casino in relation to a reportable incident; and the names of the GPEB employees who author s. 86 reports.
>
> 2. Subject to the previous paragraph, the names of casino patrons and employees - along with any associated identifying information such as addresses, telephone numbers, birth dates, driver's licence numbers, motor vehicle licence plate numbers contained in the s. 86 reports must be withheld under s. 22.

[98] Reply submission.

4.0 CONCLUSION

[102] For the reasons given above, I make the following orders:

1. Under s. 58(2)(c) of FIPPA, I require the Ministry to refuse access to the third-party personal information of casino employees and patrons in accordance with the guidelines set out above.

2. Subject to para. 1, under s. 58(2)(a) of FIPPA, I require the Ministry to give the applicant access to the remainder of the information in the s. 86 reports.

3. Under s. 58(4) of FIPPA, I specify that the Ministry is to comply with this order within 60 days, and that the parties are at liberty to apply to me with respect to any issues arising from this order or the Ministry's compliance with it.

January 31, 2008

ORIGINAL SIGNED BY

_____

David Loukidelis
Information and Privacy Commissioner
for British Columbia

OIPC File No. F04-23494