SIGNIFICANT COURT CASES

Health Information Act

➲ *Covenant Health v Alberta (Information and Privacy Commissioner),* 2014 ABQB 562 (CanLII) → A judicial review of Information and Privacy Commissioner's order that Covenant search for additional records relating to limitations on visitation rights put on the respondent Ms. McHarg. Court sets aside Commissioner's order. Covenant's refusal to allow access to certain information related to health information of McHarg's parents, personal information of parents' agent, and internal employee consultations was justified.

➲ *IMS Health Canada, Limited v. Alberta (Information and Privacy Commissioner)*, 2008 ABQB 213 (CanLII) (cited by 21 documents) → IMS Health collects prescription information from pharmacists and pharmacies for research purposes, including names of prescribing doctors. Information and Privacy Commissioner found that disclosure of prescribing physicians's names violated the Health Information Act and ordered Alberta pharmacies and pharmacists not to disclose to IMS prescriber information, unless the consent of prescriber obtained. Court sets aside Commissioner's order because it improperly expanded the scope of protection beyond the specifically defined category of individually identifying information about health services providers and would have unreasonably expanded the requirement to obtain consent.

➲ *Capital Health v. Alberta (Information and Privacy Commissioner*), 2009 ABQB 333 (CanLii)→ Capital Health

refused to make all the changes to an individual's health information that the individual requested. So, the individual submitted to Capital Health a document purporting to be a "statement of disagreement" under s.14 HIA. Capital Health found that the document did not comply with the requirements for a statement of disagreement and so did not attach it to the relevant health record and asked for a ruling from the Privacy Commissioner instead. Adjudicator found that Capital Health could accept non-compliant information and had a duty to attach the compliant parts of the document to the record. Found that Capital Health failed to meet its burden of proving it complied with its duty or failed to prove that it did not have a duty. Capital Health applied for judicial review of Adjudicator's Order. Capital Health is concerned that the Order places an onus on it to edit documents purporting to be statements of disagreement so that they comply with the legislative requirements. Court allows application and sets aside Order finding that the Adjudicator's decision was unreasonable in that it lacked adequate analysis of what was considered "reasonably practicable" under s.14(3) if a statement of disagreement contains non-compliant information; the lack of analysis created uncertainty as to the extent of the duty in similar future cases.

➲ *Lycka v. Alberta (Information and Privacy Commissioner*), 2009 ABQB 245 (CanLII) → This case looks at procedural fairness in a breach of privacy complaint and also whether the Health information Act prohibits the collection and use of individually identifying health information, with consent, for the purposes of marketing and soliciting for fundraising. Court found that use by "custodians" of individually identifying health information to market a service for a commercial purpose or to solicit money when consent has specifically been provided is allowed under s.107 of the HIA.

➲ *Medicentres Canada Inc v Alberta (Information and Privacy Commissioner),* 2014 ABQB 489 (CanLII) → Medicentres sought a stay of the OIPC's investigation about the theft of a laptop containing the health information of a large number of Medicentres' patients. Application dismissed.

➲ *Innovative Health Group Inc. v. Calgary Health Region*, 2006 ABCA 184 (CanLII) → clinic appeals an order requiring it to disclose privately-funded patient information to a health region. The clinic asserts the order breaches its patient privacy rights. The appeal is allowed. Court found CHR is not "affiliate" under HIA, and found CHR only allowed access to those parts of the files that relate to publicly-funded treatment.

Caritas Health Group v. Alberta (Information and Privacy Commissioner), 2009 ABQB 186 → A judicial review of an Adjudictaro's FOIP decision that Caritas give the complainant access to two records requested. Caritas

seeks to have that order quashed. Court found that adjudicator's decision that disclosure of personal information contained in the records would not be an unreasonable invasion of a third party's personal privacy was reasonable. Court found no basis upon which to quash the adjudicator's decision.

➲*Qualicare Health Service Corporation v. Alberta (Office of the Information and Privacy Commissioner), 2006 ABQB 515* → Case arises out of the death of a nursing home resident who was burned in a bath. This incident prompted a local newspaper to make a FOIP request for access to complaints and investigations concerning the facility and two other long-term care facilities operated by the same entity. Commissioner ordered access. Qualicare applied for judicial review. Court dismisses application for judicial review. Issue was requirements of proof under ss.20 & 25 of FOIP. Court finds there is an evidentiary burden of risk of harm, not actual harm. At no point in his reasons does he suggest that evidence of actual harm is necessary. Court supports the Privacy Commissioner's description of the "harm test" for a document to be excepted from access under ss.20(i)(a) (a reasonable expectation of harm to law enforcement) & 25(i)(c) (a reasonable expectation of harm to economic and other interests of a public body)). The three-part "harm test" is: (i) requires a clear cause and effect relationship between the disclosure of the withheld information and the harm alleged (ii) the harm that would be caused by the disclosure must be more than a hindrance or minimal interference; it must constitute damage or detriment, and (iii) the likelihood of harm must be genuine and conceivable. Commissioner correct in

PIPA (struck down – gov't is amending it, amended version not yet available)

➲ *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401,* [2013] 3 SCR 733, 2013 SCC 62 (CanLII) → Strikes down Alberta's PIPA as violating the Charter s.2(b).

- **Court of Appeal**
- *United Food and Commercial Workers, Local 401 v Alberta (Attorney General),* 2012 ABCA 130 (CanLII) - 2012-04-30 → this is the one which was appealed to the SCC – Slatter & McDonald JJ, allowed the appeal in part, but only to the extent that the remedy was varied. Agreed that PIPA violated the Charter s.2(b) and granted the Union a constitutional exemption from the application of *PIPA.*
  United Food and Commercial Workers, Local 401 v Alberta (Attorney General), 2012 ABCA 244 (CanLII) - 2012-08-16
- **Court of Queen's Bench**
  United Food and Commercial Workers, Local 401 v. Alberta (Information and Privacy Commissioner), 2011 ABQB 415 (CanLII) - 2011-06-30 → Goss, J. set aside the decision of the OIPC. Found that PIPA violated the Union's rights under s. 2(*b*) of the *Charter*.
- **Information and Privacy Commissioner**
  Order P2008-008, 2009 CanLII 90942 (AB OIPC), 2009 CanLII 90942 → concluded that the Union's collection, use and disclosure of the information was not authorized by *PIPA*.

➲ *Leon's Furniture Ltd. v. Alberta (Information and Privacy Commissioner)* [2011] ABCA 94 (CANLII) →
Leave to appeal to SCC refused ([2011] S.C.C.A. No. 260). Leon's recorded driver's licence and vehicle plate numbers when customers picked up furniture. Customer made complaint to Privacy Commissioner. Commissioner found that plate numbers were personal information, collection of it went beyond what was necessary to prevent fraud, and that by collecting such information Leon's breached PIPA. Ordered Leon's to cease recording drivers' license numbers and license plate numbers and to destroy all drivers' license and license plate numbers recorded. Commissioner's order upheld at ABQB but quashed by this Court. "Personal information" means information about an identifiable individual; licence plate number is not personal information because it is linked to a vehicle, not a person, and it is not in any way private as it was displayed on a vehicle.

➲ *Penny Lane Entertainment Group v. Alberta (Information and Privacy Commissioner),* 2009 ABQB 140 (CanLII) → Judicial review of Commissioners' order to destroy information gathered by scanning the driver's licenses of patrons to a nightclub and cease their practice of scanning driver's licenses of patrons. Commissioner had found that collection of this information contravened s. 11 (reasonable purpose) of PIPA. Court confirms Commissioner's decision.

➲*R. v. Cole,* [2012] 3 SCR 34, 2012 SCC 53 (CanLII) → work system privacy case. School teacher had reasonable expectation of privacy in a work-issued laptop but employer also has a duty to provide a safe and harassment free workplace and thus needs to monitor and control their data. There is an expectation of privacy but it is limited because it arises from personal use of a work system.

➲ *Lougheed Imports Ltd. (West Coast Mazda) v. United Food and Commercial Workers International Union, Local 1518,* 2010 CanLII 62482 (BC LRB) → A BC Labour Relations Board decision. Employer justified in terminating employment of two employees based on Facebook postings, including offensive and egregious comments towards supervisors, by the employees.

➲ *Alberta Union of Provincial Employees v. Alberta,* 2009 ABQB 208 (CanLII) → Court upheld the dismissal of an employee. Gounds for dismissal were employee's expression of contempt for co-workers and management on her personal blog.

➲ *Schindler Elevator Corporation (Re),* 2012 BCIPC 25 (CanLII) (Order P12-01) → A BC Privacy Commissioner decision. Schindler installed a GPS and engine status system in its work vehicles which are used by its mechanics. Complaint made by employees who argued that use of the system contravenes BC's PIPA. Issue was whether BC's PIPA authorized employer to Employer to collect, use and disclose information generated by the Fleet Complete system for, among other things, the purpose of ensuring that its employees keep their work hours, do not use vehicles for personal use, and drive safely and lawfully. Commissioner found Schindler authorized to collect and use information from the system; system was not used covertly.

➲ *ThyssenKrupp Elevator (Canada) Limited (Re),* 2013 BCIPC 24 (CanLII) (Order P13-02) → Another BC Privacy

Commissioner decision. It was released contemporaneously with Order P13-01 [Kone]. TKE installed monitoring devices in its company vehicles which are assigned to specific employees. Commissioner found TKE permitted to collect and use the information to manage its employment relationships but that TKE had not properly notified the complainant about its collection, uses and purposes for this information thus breaching BC's PIPA ss.13 & 16.

➲ *Kone Inc (Re),* 2013 BCIPC 23 (CanLII) [Order P13-01] → The third "BC elevator company" Privacy Commissioner decision. Also a BC PIPA complaint involving analogous technology as Schindler and Thyssenkrupp. KONE collected and used GPS information from cellular phones issued to its service mechanic employees. KONE employees complained this is not permitted under PIPA. Commissioner found that KONE is permitted to collect and use the information in the manner and for the purposes identified by KONE.

FOIP

➲ *Imperial Oil Limited v Alberta (Information and Privacy Commissioner),* 2014 ABCA 231 (CanLII) → settlement privilege in the context of FOIP re-affirmed. Privacy Commissioner ordered disclosure of a mediated confidential settlement agreement. Court found agreement was exempt from disclosure as it satisfied preconditions for non-disclosure in s.16 of FOIPPA. Imperial Oil had supplied protected information in confidence and disclosure would likely harm its business interest.

➲ *Oleynik v. University of Calgary,* 2012 ABQB 189 (CanLII) → This decision was affirmed in Oleynik v. University of Calgary, 2013 ABCA 105 (CanLII). Linda reviewed the 2012 ABQB 189 case in her May 15, 2012 ABLawg case review. About access to information request for emails. Dr. Oleynik was applicant in this judicial review of Adjudicator's decision that the University had conducted a reasonable search for responsive records was upheld.

➲ *University of Alberta v. Alberta (Information and Privacy Commissioner),* 2012 ABQB 247 (CanLII) → Linda also reviewed this case in her May 15, 2012 ABLawg case review. Dr. Oleynik was a respondent in two judicial reviews: this one & *Association of Academic Staff of the University of Alberta v. University of Alberta*, 2012 ABQB 248 (CanLII).

➲ *Association of Academic Staff of the University of Alberta v University of Alberta*, 2012 ABQB 248 (CanLII) → the third case reviewed by Linda in her May 15, 2012 ABLawg case review.

➲ *Calgary Police Service v. Alberta (Information and Privacy Commissioner)*, 2010 ABQB 82 (CanLII) (cited by 12 documents) → Judicial review of Commissioner's order that disciplinary proceedings be disclosed as public scrutiny outweighed factors against disclosure. Court partially overturns order. Issue is whether disclosure is an unreasonable invasion of personal privacy given s.17(5)(a) "the desirability of public scrutiny". Court found there was no requirement to disclose unproven or withdrawn allegations, or decisions resulting in employment sanctions due to a breach of CPS regulations, but decisions resulting in sanctions due to convictions for criminal or provincial offences were disclosable. Note: much of the decision is about the proper standard of review for judicial reviews of the privacy commissioner's decision which is being appealed.

➲ *Edmonton Police Service v. Alberta (Information and Privacy Commissioner),* 2009 ABQB 593 (CanLII) →

the need for public scrutiny as a factor in determining whether an invasion of personal privacy is unreasonable. Candidate for position of Chief of Police sought all police records regarding himself. Police Service provided some but not all emails. Court upholds that part of the Commissioner's order to disclose the information severed from the emails but returns the portion directing the Police to search the backup records for reconsideration.

➲ *Edmonton Police Service v. Alberta (Information and Privacy Commissioner) 2012 ABQB 595* → Application by the Edmonton Police Service for judicial review of Commisioner's order to disclose portions of a report; report was about enhancing ethics and professionalism in the Police Service. Criminal Trial Lawyers' Association made an access request for the report. Portions in question were those containing information supplied by several outside entities. Court upholds Commissioner's order. Court found that the Commissioner's conclusion that the information in question was not supplied in confidence was a reasonable decision based on the law and evidence.

☒ *[Is a procedural case] Edmonton Police Service v. Alberta (Information and Privacy Commissioner) 2009 ABQB 268* → Application by Edmonton Police Service for judicial review of disclosure order dismissed — Information and Privacy Commissioner ordered applicant to conduct search of information technology branch in connection with disclosure request — Applicant submitted order was void ab initio due to Commissioner's failure to conduct inquiry within 90 days pursuant to s. 69(6) of FOIPPA — No need to remit issue of jurisdiction to Commissioner, as it had implicitly been considered in decision to proceed beyond timeline — Commissioner reasonably found that timeline provision was directory rather than mandatory — Freedom of Information and Protection of Privacy Act, s. 69(6).

➲ *Edmonton Police Commission v. Alberta (Information and Privacy Commissioner)* 2011 ABQB 291 → Judicial review arising out of request by Criminal Trial Lawyers Association of Alberta to the EPC for records relating to investigations of complaints made about EPC officers. EPC provided heavily redacted record but did not notify officers. CTLA brought complaint to Privacy Commissioner. Commissioner ordered EPC to make more fulsome disclosure. EPC applies for judicial review of order. Court allows application and quashes Commissioners order. Court finds Commissioner should have compelled EPC to give notice to affected officers that record was being disclosed, but Commissioner did not and so procedural fairness was undermined; s.30 requires persons whose privacy would be compromised by disclosure of the records sought to be notified.

➲ *Business Watch International Inc. v. Alberta (Information and Privacy Commissioner),* 2009 ABQB 10 (CanLII) → Originally a test case to the Information and Privacy Commissioner. This case is judicial review of

Commissioner's order that the City of Edmonton destroy BWI's database. City of Edmonton has Business Licence Bylaw which requires pawnshops to collect from pawnors personal information about themselves (including name, date of birth, gender, eye colour and hair colour). That information was put into a database run by BWI and provided to the Edmonton Police Service. Commissioner found that the City did not have the authority to require store owners to provide that information to BWI and that the City didn't take reasonable steps to safeguard the information. Commissioner ordered the City to destroy BWI's database. Court quashed Commissioner's orders.

➲ *Ontario (Public Safety and Security) v. Criminal Lawyers' Association,* [2010] 1 SCR 815, 2010 SCC 23 (CanLII) → Ontario's FIPPA is similar to Alberta's FOIP. The constitutional issue to be decided was whether s.2(b) of the Charter protects access to government-held information for which law enforcement or solicitor-client privilege are claimed and, if so, in what circumstances. Court finds Section 2(b) of Charter guarantees freedom of expression but it does not guarantee access to all documents in government hands. Access to documents in government hands constitutionally protected only where it was shown to be a necessary precondition of meaningful expression, does not encroach on protected privileges, and is compatible with the function of the institution concerned. Court found s.2(b) not engaged because CTLA did not establish that access was necessary to permit meaningful debate and discussion on a matter of public interest. CTLA had sought Crown records relating to a murder case, including two documents containing legal advice and a report looking into alleged police misconduct.

➲ *Calgary Board of Education v Alberta (Office of the Information and Privacy Commissioner)*, 2014 ABQB 189 (CanLII) → CBE tried to use information in McBain's file about harassment complaint to impugn his credibility in unrelated proceedings. CBE seeks judicial review of a decision of the Office of the Information and Privacy Commissioner that CBE had used and disclosed McBain's personal information contrary to FOIP but did not fail to protect it; collection was inconsistent with the purpose for which it was collected and did not have a reasonable and direct connection to that purpose. Court upholds Commissioners decision finding it was reasonable. Commissioner's interpretation of "use" did not cripple public bodies' ability to routinely handle information. Commissioner also interpreted s.40 as meaning that a public body should only make disclosures of its own accord that relate specifically to its own, or the government's, involvement as a party in the proceedings.

➲ *Mount Royal University v. Carter, 2011 ABQB 28* → Mr. Carter requested access to information held by the University. MRU granted access to some records but not others citing FOIP ss.17 (Disclosure harmful to

personal privacy) & 18 (Disclosure harmful to individual or public safety). Mr. Carter requested review by Privacy Commissioner. Adjudicator found that neither ss.17 or 18 of *F.O.I.P.* applied. MRU seeks judicial review of Adjudicator's decision. Court denies MRU's application for judicial review. Court found that Adjudicator's analysis regarding employees of public bodies was reasonable. The Adjudicator had concluded that not all information about individuals is information to which s.17 (disclosure harmful to personal privacy) applies. Adjudicator found that information about an employee acting as a representative of a public body was information about the public body, and not information about the employee as an identifiable individual, because the employee is acting as an agent for the public body. However, if there is information of a personal character about an employee of a public body then s.17 may apply to that information.

PIPEDA

➲ *R. v. Spencer*, 2014 SCC 43 (CanLII) → long-awaited decision regarding legality of voluntary, warrantless disclosure of basic subscriber information held by an Internet Service Provider (ISP) to law enforcement. Case is in the context of criminal proceedings but much of the reasoning centred on PIPEDA. Court dismissed the appeal and ordered a new trial. Court confirmed that Canadians have a reasonable expectation of privacy in their online activities, including an expectation of anonymity as regards user names and other personal identifiers held by ISPs. Under PIPEDA, a police investigation is not enough "lawful authority" to get personal information from an ISP simply under PIPEDA; they still need a warrant if they want this information. [**NB: Despite this ruling, the government is continuing with its Bill S-4 (Digital Privacy Act Bill) which would amend PIPEDA and allow for such warrantless access to subscriber information and provide immunity from prosecution for service providers who voluntarily hand over such information].

➲ *R v Patrick*, [2009] SCC 17 (cited in Spencer) → Cited in R. v. Spencer, among others. Issue was whether P. had a reasonable expectation of privacy in the items taken from his garbage by police who suspected P of production of ecstacy. Court assessed the reasonableness of the claimed privacy interest by looking at the "totality of the circumstances". Majority found there was no privacy interest at time garbage was seized. Court concluded that no *Charter* violation occurred, but disagreeing with the characterization of the privacy issues at stake. Dissenting found a diminished expectation of privacy but that state had reasonable suspicion that a criminal offence had been or was likely to be committed before conducting the search.

➲ *Canadian National Railway Company v Teamsters Canadian Rail Conference,* 2014 CanLII 15954 (CA LA) → Video Surveillance case. Federal Labour Arbitration decision on whether CNR breached Collective Agreement and PIPEDA by installing video surveillance following a complaint of harassment. Video installed without giving notice nor for purpose of investigating a breach of an agreement or contravention of laws. Arbitrator found company violated both Agreement and PIPEDA.

➲ *Eastmond v. Canadian Pacific Railway,* 2004 FC 852 (CanLII) [no pdf, just text, on CANLII] → Another workplace video surveillance case. CPR installed six digital video recording surveillance cameras. Did CP breach PIPEDA? Court looked at the four-part test adopted in an earlier labour arbitration case (*Re Canadian Pacific Ltd. and Brotherhood of Maintenance of Way Employees* (1996), 59 L.A.C. (4th) 111) to balance privacy interests of employees with legitimate business interests of employers. Court concluded that CP's purposes for installing cameras was appropriate given numerous past incidents which justified the need for surveillance. PIPEDA not breached. [**NB: Not followed in Order P12-01; Schindler Elevator Corp. (Re), but followed in two Canadian Labour Arbitration decisions and cited in eleven other instances.]

➲ *Wansink v. TELUS Communications Inc.,* [2007] 4 FCR 368, 2007 FCA 21 (CanLII) → Voice recognition technology to allow TELUS' employees to access and use internal computer network. Among the issues were: whether the collection, use or disclosure of the voice characteristics was "only for purposes that a reasonable person would consider are appropriate in the circumstances" (s.5(3) PIPEDA), and whether Telus could discipline employees who withhold their consent for collection of the voiceprint. Federal Court found purpose for which voiceprint collected would be considered appropriate by reasonable person and employees' consent not necessary because s.7(1)(a) PIPEDA exception. Appeal dismissed; Commissioner and Federal Court findings upheld.

➲ *Chitrakar v. Bell TV,* 2013 FC 1103 (CanLII) → An application by C. for damages pursuant to s.14(1) PIPEDA. Bell inserting C's signature on contract and accessing C's credit report but unauthorized to do so. C's complaint to the Privacy Commissioner was determined to be well-founded. Court awarding C damages of $10,000, exemplary damages of $10,000 for Bell's conduct at the time of the breach of the privacy rights, Bell's dealings with C, its reactions to the Privacy Commissioner and her recommendations, and its failure to take these proceedings seriously.

➲ *Henry v. Bell Mobility,* 2014 FC 555 (CanLII) → H seeking damages because Bell Mobility revealed certain information about his cellphone account to an unauthorized third person. Bell Mobility defended the action. Only issue was quantum of damages as Bell conceded liability. Court distinguishes Chitrakar (primarily based on Bell's actions in this case following the breach, including their acknowledgement that H entitled to damages) and awards $2500.

[22] The following chart provides a summary of the cases decided in this Court dealing with breach of privacy:

AUTHORITY	NATURE OF BREACH	DAMAGES
Stevens v. SNF Maritime Metal Inc., 2010 FC 1137 (CanLII)	Disclosure of financial information	NIL
Randall v. Nubodys Fitness Centres, 2010 FC 681 (CanLII)	Disclosure of usage of fitness facility to employer	NIL
Biron v. RBC Royal Bank, 2012 FC 1095 (CanLII)	Disclosure of credit card statements in divorce proceeding	$2,500 + costs
Townsend v. SunLife Financial, 2012 FC 550 (CanLII)	Disclosure of medical information to a third party	NIL
Girao v Zarek Taylor Grossman Hanrahan LLP, 2011 FC 1070 (CanLII)	Disclosure of personal information relating to medical conditions	$1,500 + $500 for costs
Landry v. Royal Bank of Canada, 2011 FC 687 (CanLII)	Disclosure of financial information in a divorce proceeding	$4,500 + costs
Nammo v. TransUnion of Canada Inc., 2010 FC 1284 (CanLII)	Disclosure of inaccurate personal information to a bank causing credit issues	$5,000 + $1,000 for costs

Access to Information Act & Privacy Act

➲ *Dagg v. Canada (Minister of Finance),* [1997] 2 SCR 403, 1997 CanLII 358 (SCC) → Issue was whether the information in logs of names, id numbers, and signatures or employees accessing the workplace on weekends is "personal information" within the meaning of s.3 Privacy Act. Personal identifying features deleted from information given in response to access for information request. Court divided. Majority held log is personal information and should have been disclosed. Court sets out principle that Privacy Act and Access to Information Act are meant to be a "seamless code" and are to be construed harmoniously according to a "parallel interpretation model" (at paras. 45, 51)

➲ *Canada (Information Commissioner) v. Canada (Commissioner of RCMP),* 2003 SCC 8 → The Canadian Supreme Court has described the two laws [Right to Information & Privacy] as a "seamless code with complementary provisions that can and should be interpreted harmoniously."

➲ *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)* (F.C.A.), 2006 FCA 157 → Definition of "personal information" in Privacy Act, s. 3 interpreted. Appeal allowed. Held that air traffic control (ATC) communications do not meet the requirements for exemption from disclosure under Access to Information Act, s. 20(1)(b) and that Federal Court erred in concluding that the information requested was "personal information" under s.3 Privacy Act. "Personal information" to be given a broad and generous interpretation. Leave to appeal to SCC refused ([2006] S.C.C.A. No. 259)

➲ *Gordon v. Canada (Health),* 2008 FC 258 (CanLII)→ information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.

➲ *John Doe v Ontario (Finance),* 2014 SCC 36 (CanLII) → case about Ontario's freedom of information legislation (*Freedom of Information and Protection of Privacy Act* (FIPPA)). Alberta has similar provisions about "advice" (s.24). SCC found that policy options which public servants provided to the provincial government are exempt from disclosure as "advice or recommendations" under Ontario's legislation. The words "advice" and "recommendations" are distinct and don't have the same meaning. Commentators have suggested that this decision will likely broaden the scope of information exempted from public access and limit public scrutiny of government policy development and decision-making.

➲ *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, [2006] 1 SCR 441, 2006 SCC 13 (CanLII) → Originated as an application by a third party (Heinz Co.) contesting disclosure of certain documents. Canadian Food Inspection Agency received request under Access Act for records pertaining to Heinz some of which may have contained confidential business or scientific information. CFIA decided to disclose records subject to certain redactions. Heinz commenced a review proceeding under s.44 Access Act arguing two exemptions to disclosure (s.20 confidential business information and s.19 personal information relating to individuals). The application judge concluded that the company could raise the s. 19 exemption on a s. 44 review and ordered the severance of certain records containing personal information. The Federal Court of Appeal upheld the decision. SCC Majority upholds FCA decision concluding that a third party can raise exemption for personal information on s. 44 review. Dissent disagreed. Majority noted that the combined purpose of the Access Act Privacy Act is to strike a careful balance between privacy rights and the right of access to information but that the Acts afford greater protection to personal information.

➲ *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, [2011] 2 SCR 306, 2011 SCC 25 (CanLII) → Decision dealing with the scope of access rights to Ministerial records under the Access to Info Act . Gov't refused to give Information Commissioner of Canada certain records located within the PMO's Office and other Minister's offices. Court refuses to order disclosure. Court finds "under the control" from s. 4(1) of the Act must be given a broad and liberal meaning in order to create a meaningful right of access to government information and that physical control over a document is not determinative of the issue. Also outlined a two-step test to decide whether access to be granted, including the reasonable expectation of access. The reasonable expectation test is objective.

Privacy Act

➲ *Lavigne v. Canada (Office of the Commissioner of Official Languages),* [2002] 2 SCR 773, 2002 SCC 53 (CanLII) → L appeals Privacy Commissioners finding that OCL correctly refused access to some information in investigative files held by the OCL. Court found COL did not show that it was reasonable to maintain confidentiality. Court makes the statement that the Privacy Act is fundamental to our legal system, para. 24 "It has two major objectives. Its aims are, first, to protect personal information held by government institutions, and second, to provide individuals with a right of access to personal information about themselves (s.2)." And at para. 25: "The Privacy Act is a reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society."

➲ *Agropur (Natrel) v. Milk and Bread Drivers, Dairy Employees, Caterers and Allied Employees (Teamsters*

Local Union No. 647), 2008 CanLII 66624 (ON LA) → An Ontario Labour Arbitration case. Union seeks to stop the employer from introducing a biometric time management system that uses fingertip scan. Issue is whether employer's plan intrudes on employee privacy rights in a way that is unreasonable. Arbitrator concluded that proper method of analysis is: to decide if employer's actions are reasonable, balance employee's interest in privacy against the employer's reasons for requiring an infringement of that privacy. A key tool in assessing whether the infringement of privacy is must be proven). Arbitrator found installation of scan met reasonableness test.

➲ *Entrop v. Imperial Oil Limited*, 2000 CanLII 16800 (ON CA) → Is an Ontario Human Rights case involving workplace drug & alcohol testing in unionized workplace. Employer's alcohol and drug testing policy requiring employees in safety-sensitive positions to disclose past substance-abuse problems. Those who disclosed would then be subject to unannounced, random alcohol and drug testing. Employee in safety-sensitive position reassigned after disclosing past alcohol abuse; employee filed discrimination complaint on basis of handicap. Court sets aside Board's conclusion that random alcohol testing for employees in safety-sensitive positions violated the Code. Court found that such testing was a "bona fide occupational requirement" in this case and not a violation as long as the sanction for an employee testing positive is tailored to the employee's circumstances.

➲ *Communications, Energy and Paperworkers Union of Canada, Local 30 v. Irving Pulp & Paper, Ltd.,* [2013] 2 SCR 458, 2013 SCC 34 (CanLII)→ another workplace alcohol & drug testing in union context. Charter & Labour Relations acts. Arbitration board found employer exceeded the scope of its management rights by imposing random alcohol testing in the absence of evidence of a workplace problem with alcohol use. Court summarizes arbitral jurisprudence; although not binding on the SCC it is of significance: "A substantial body of arbitral jurisprudence has developed around the unilateral exercise of management rights in a safety context, resulting in a carefully calibrated "balancing of interests" proportionality approach." at para. 4. "This approach has resulted in a consistent arbitral jurisprudence whereby arbitrators have found that when a workplace is dangerous, an employer can test an individual employee if there is reasonable cause to believe that the employee was impaired while on duty, was involved in a workplace accident or incident, or was returning to work after treatment for substance abuse. But a unilaterally imposed policy of mandatory, random and unannounced testing for *all* employees in a dangerous workplace has been overwhelmingly rejected by arbitrators as an unjustified affront to the dignity and privacy of employees unless there is reasonable cause, such as a general problem of substance abuse in the workplace." at para. 5. SCC majority finds Board's decision reasonable.

➲ *Unifor, Local 707A v Suncor Energy Inc,* 2014 CanLII 23034 (AB GAA) → Recent Alberta Labour Arbitration Board decision. Cites Irving Pulp & Paper. Union filed grievance against the introduction by Suncor of

random alcohol and drug testing, using urinalysis, at Suncor operations in the Athabasca oil sands. Board allowed the grievance and finds Suncor's 2012 testing Policy an unreasonable exercise of the Employer's management rights. Board found that urinalysis test is unable to provide the specificity of information necessary to determine impairment or influence by drugs and that "red flagging" an employee who has recently used drugs does not meet legitimate business interest threshold required to justify the test's intrusion into privacy.

➲ Alberta (Human Rights and Citizenship Commission) v. Kellogg Brown & Root (Canada) Company, 2007 ABCA 426 (CanLII) → Is a human rights decision. Looks at whether a pre-employment drug testing policy discriminates against casual cannabis users on the basis of perceived disability. Hiring policy in place that required all applicants for non-unionized positions to pass a post-offer/pre-employment drug test before hiring. If the applicant failed this test, he would not be hired, but would be eligible for reconsideration six months after the date of the failed test. The Alberta Court of Appeal allowed KBR's appeal confirming that KBR did not terminate Chiasson's employment based on a drug addiction, because he was only a casual user of cannabis, or on the perception that he is drug addicted. Court found the purpose of the drug-testing policy is to minimize workplace accidents by prohibiting impairment at the workplace. Court found that cannabis use may negatively affect an employee's ability to function in a potentially dangerous work enviroment where safety is a primary concern, and so the drug-testing policy is clearly connected to its purpose. Application for leave to appeal to SCC dismissed.

Charter Right to Privacy (s.8, s.24)

➲ *R. v. A.M.,* [2008] 1 SCR 569, 2008 SCC 19 (CanLII) → Showing the evolution of the concept of "privacy" in the Charter context.
➲ *R. v. Tessling*, [2004] 3 SCR 432, 2004 SCC 67 (CanLII) → ""
➲ *R. v. Plant,* [1993] 3 SCR 281, 1993 CanLII 70 (SCC) → ""

➲ *R. v. Vu*, 2013 SCC 60 (CanLII) → limits ability of police to search computers if warrant not specifically mentions computers. Police obtained warrant authorizing search of residence. Searched computers and cell phone they found in residence. Trial judge found accused's s. 8 Charter rights were violated and excluded evidence, resulting in acquittal. Court of Appeal set aside acquittal and ordered new trial. SCC concludes that if police come across computer while conducting warranted search but warrant does not give them specific, prior authorization to search computers, they must obtain further authorization before searching. Court finds that while Charter rights were violated the violation was not serious and there was clear societal interest in adjudicating the case on its merits, so evidence should not be excluded. New trial ordered.

➲ *Fraser v. P.S.S.R.B.,* [1985] 2 SCR 455, 1985 CanLII 14 (SCC) → Issue was whether Adjudicator erred in law when he confirmed the discharge of a federal public servant who publicly expressed views highly critical of the Government. Key is to balance right of the individual to speak freely and their duty, as public servant, to fulfil their functions properly. Court found Adjudicator did not err.

➲ *R. v. Fearon*, 2013 ONCA 106 (CanLII) → on appeal to the SCC (Case#35298 – appeal heard May 23/14). Search by police of suspect's cellphone following arrest for a robbery. Issues include whether search of phone breached s. 8 of the Charter, whether the legal framework governing searches incident to arrest extends to cell-phones and whether a cell phone exception should be made to the common law power of police to search incident to arrest.

➲ *R. v. Fearon,* 2014 SCC 77 → Decision released December 11, 2014. The majority of the SCC has found that warrantless cell phone searches are allowed during a police arrest and do not violate Charter rights against unreasonable search and seizure if conducted properly. The Court set out four conditions in order for the search of a cell phone or similar device incidental to arrest to comply with s. 8 Charter: (i) The arrest must be lawful;

(ii) The search must be "truly incidental" and not the object of the arrest, and this condition must be strictly applied; (iii) The nature and extent of the search must be tailored to its purpose (limited to areas where evidence is likely to be found, such as text messages, e-mails, and call logs); (iv) Police must record detailed notes about the search, including applications opened and the search duration. The decision comes with strong minority dissent.

Re: Note on *R. v. Fearon*

Source: http://www.canadianlawyermag.com/legalfeeds/tag/supreme-court-of-canada.html

A post on Osgoode Hall Law School's The Court blog, meanwhile, points to a contrasting SCC decision in November 2013, *R. v. Vu*, which deals with incidental computer searches in the course of an investigation that has been authorized by warrant.

In the incident, police obtained a warrant to search a residence they suspected was a grow-op, but the warrant did not include specific authorization to search computer files.

The judgment, again written by Cromwell, took a markedly different approach than today's ruling. In Vu, the court determined that law enforcement is required to obtain judicial authorization prior to computer or cell phone searches.

Seemingly anticipating the confusion, however, the ruling states the law with respect to warranted searches does not "disturb the law that applies when a computer or cellular phone is searched incident to arrest or where exigent circumstances justify a warrantless search."

Another contrasting decision was highlight by criminal lawyer Sean Robichaud on Twitter: "police need a warrant to search a person's company computer (R. v. Cole) but not for their personal phone (R. v. Fearon). Huh?"

➲ *R. v. TELUS Communications Co.,* [2013] 2 SCR 3, 2013 SCC 16 (CanLII) → Police obtaining a general warrant to require Telus to provide copies of any stored text messages sent or received by two Telus subscribers over a two-week period. Telus applied to have warrant quashed arguing wire tap authorization was required. Issue was whether the general warrant power can authorize the prospective production of future text messages from a service provider's computer. Answer is no. Court quashes warrant. Other provisions would have been available.

➲ *Jones v. Tsige, 2012* ONCA 32 → redefines privacy law in Canada by recognizing for the first time a tort of "inclusion upon seclusion", at least in Ontario. Sandra Jones, a customer and employee of BMO, became aware that another bank employee, Winnie Tsige, had snooped in Jones' personal financial records at the bank 174 times over a period of four years; Jones and Tsige apparently did not know each other. Jones' claim was dismissed in the first instance because the Motions Judge found the common law in Ontario did not recognize a tort of invasion of privacy. The Court of Appeal found that the time had come to recognize a common law tort of "intrusion upon seclusion" and awarded $10,000 damages to Ms. Jones but no punitive damages. The Court set out four required elements of the action for "intrusion upon seclusion": (i) defendant's conduct must be intentional (including recklessness); (ii) defendant must have invaded the plaintiff's private affairs or concerns without lawful justification; (iii) a reasonable person must regard the invasion as highly offensive and causing distress, humiliation or anguish; and (iv) proof of harm to a recognized economic interest is not an element of the cause of action so damages would generally be a modest conventional sum (i.e. damages should normally fall in a range up to $20,000).

Standard of Review for Judicial Reviews

➲ *Stubicar v. Alberta (Office of the Information and Privacy Commissioner),* 2008 ABCA 357 (CanLII) → This case is cited in most of the judicial review decisions regarding the appropriate standard of review, specifically under FOIP. Calgary Health Region provided medical records of Stubicar's deceased husband to her with some redactions but Stubicar asked for inquiry into how CHR handled her request. Privacy Commissioner conducted formal inquiry and found redaction issue was moot and that CHR had complied with their s.10 duty to "...make every reasonable effort to assist the applicant and to respond to each applicant openly, accurately and completely...". Stubicar applied for judicial review of Commissioner's decision. At the judicial review hearing, Stubicar complained that ex parte submissions were made by CHR to influence Commissioner. CHR denied this, filed affidavit to that effect, and gave Stubicar opportunity to cross-examine. But, before Stubicar was served with the affidavit, ABQB judge issued his decision dismissing her judicial review application. Stubicar applied to have her application re-opened. ABQB judge refused. Court dismisses Stubicar's appeal and finds that the reviewing judge did not breach the rules of natural justice. Nothing further was required in the circumstances other than giving Stubicar the opportunity to cross-examine on the affidavit and to make submissions.

➲*University of Alberta v. Alberta (Information and Privacy Commissioner)* 2009 ABQB 112 (CanLII) → cites many judicial review decisions as to appropriate standard of review. Application by UofA for judicial review of an order issued by the Privacy Commissioner. Commissioner found that UofA contravened FOIP (s.4) by publishing a statistical summary of academic staff's teaching effectiveness, number of published papers and merit increment recommendations. Data for summary was provided by faculty in their annual reports. AB, a professor, filed a complaint alleging that the statistical summary violated his privacy because it contained a merit increment recommendation through which he was individually identifiable. Court dismisses UofA's application for judicial review. Court found that the Commissioner's lack of reasons or written analysis did not constitute an error. Court found that Commissioner's decision was reasonable; the statistical summary was not research or teaching information per se, but it contained AB's personal information and AB was an identifiable individual as a result of the summary.

➲ *University of Alberta v. Pylypiuk, 2002 ABQB 22 (CanLII), 310 A.R. 300* → one of the earlier decisions on

standard of review for privacy decisions. Court found that the Commissioner had no greater expertise than the Court in the interpretation and application of FOIP and the social values underlying it and its application. Note that the Stubicar decision has changed this to recognize the Commissioner's expertise in interpreting and applying privacy legislation. There are three reported Alberta cases concerning the standard of review of a decision of the Privacy Commissioner. In two, *University of Alberta v. Pylypiuk* and *Alberta (Attorney General) v. Krushell* the Court applied a standard of correctness, but in *Shields v. Information and Privacy Commissioner* the standard was reasonableness. There is no single standard of review applicable to a particular tribunal, or for all decisions within a particular category.

➲ *Dunsmuir v. New Brunswick*, [2008] 1 SCR 190, 2008 SCC 9 (CanLII) → leading case on proper approach to judicial reviews of administrative decision makers. Two standards: correctness and reasonableness.

➲ *Leahy v. Canada (Citizenship and Immigration)*, 2012 FCA 227 (CanLII) → The review of a government institution's decision not to disclose personal information is a two-fold process. The first, does the withheld information fall within the description of exempt information under the applicable provisions, is to be reviewed on a standard of correctness. The second, if exempt, whether the government appropriately exercised its discretion not to disclose said information, to be reviewed on a standard of reasonableness.

➲ *Minister of Citizenship and Immigration v. Khosa* 2009 SCC 12 (CanLII) → an important Canadian case for defining a "reasonableness" standard of review. At para. 59, Binnie, J. writing for the court: "Reasonableness is a single standard that takes its colour from the context. . . . Where the reasonableness standard applies, it requires deference. Reviewing courts cannot substitute their own appreciation of the appropriate solution, but must rather determine if the outcome falls within "a range of possible, acceptable outcomes which are defensible in respect of the facts and law" (*Dunsmuir*, at para. 47). There might be more than one reasonable outcome. However, as long as the process and the outcome fit comfortably with the principles of justification, transparency and intelligibility, it is not open to a reviewing court to substitute its own view of a preferable outcome."

➲ *Alberta (Information and Privacy Commissioner) v. Alberta Teachers' Association*, [2011] 3 SCR 654, 2011 SCC 61 (CanLII) → - At issue was the Information and Privacy Commissioner's interpretation of its enabling statute including the appropriate standard of review. The Court found that the adjudicator's decision was subject to judicial review on a reasonableness standard. Court discussed the indicators of correctness and reasonableness explaining that true questions of jurisdiction are rare and that a standard or reasonableness should be presumed in situations where a tribunal is interpreting its home statute or other statutes with which it is familiar.