

MANAGING EMPLOYEE PERSONAL INFORMATION: CROSS BORDER and OUTSOURCING CHALLENGES

PRIVATE SECTOR PRIVACY IN A CHANGING WORLD
PIPA CONFERENCE 2007
Break-Out Session 5A
September 21, 2007

Tamara L. Hunter, Davis LLP
Earl G. Phillips, McCarthy Tétrault LLP

DAVIS
LLP

LEGAL ADVISORS
SINCE 1892

McCarthy
Tétrault

MCCARTHY.CA

Scenario #1

BC firm offering employees an outside, computer-based fitness service provider.

You are the Director of Human Resources for a large accounting firm in British Columbia. One of the firm's goals is to improve the health and fitness of employees and their families in order to reduce the average number of sick days per employee and to minimize extended health benefit claims. A service provider ("Fitness Plus Inc.") has suggested the firm utilize Fitness Plus Inc.'s computer-based services to offer a new optional free benefit to employees in the form of a personalized fitness plan for the employees, as well as for dependents covered by the extended health program. Your firm would pay a flat fee for this service based on the total number of people authorized to use this system (who would then access this system via a unique password). In order to receive this benefit, employees and their dependants would access this system on-line and would then be asked to provide background information regarding their age, gender, height, weight, health conditions, level of existing fitness, sport/activity preferences, smoking history, etc. In order to promote, set-up and administer this system for your firm's employees, Fitness Plus Inc. has requested a list of the names and positions of all employees and the names of the eligible dependents associated with each employee.

Questions arising:

- Can your firm provide the list of employees and eligible dependents to Fitness Plus Inc. without first obtaining consent from the individuals (or providing notice to the employees)?
- Is this "employee personal information"?
- Since employees and their dependents are not obliged to use this computerized fitness plan program and will only be providing their background information if they choose to receive this benefit, can your firm simply notify employees of the opportunity to use the service without bearing any further responsibility or being further involved?
- Is there any privacy law issue if Fitness Plus Inc. gives the firm's management a report on the degree to which the program is being used by employees?

THE KIND OF INFORMATION

- What is “personal information” (“PI”)?
- This is not just “contact information”
- This is not “employee personal information”

WHAT IS BEING DONE WITH THE PI?

- The firm and the service provider are “organizations”
- What PI is each “organization”:
 - Collecting?
 - Using?
 - Disclosing?

THE FIRM AND CONSENT

- Firm collects PI from employees for certain purposes
- Using and disclosing for other purposes
- Consent of individual employees AND dependents required
- Disclosure of PI by firm to service provider creates obligations for firm

Scenario #1

THE SERVICE PROVIDER AND NOTICE

- Service provider collecting and using PI
- Give notice of purposes for collection and obtain consent for use and disclosure
- Collect only what a reasonable person would consider appropriate
- Use and disclose for purposes stated when collected

6

Scenario #1

REPORTING BACK TO THE FIRM

- If PI included
 - Covered by notice of purposes, or
 - Consent
- If PI not included
 - No notice or consent required

7

Scenario #1

RECOMMENDED PROCESS

- Offer and promote as optional service to employees
- Employees voluntarily participate and give written consent to service provider
- PI collected by service provider from employees
 - Firm stays out of it

8

Scenario #1

RECOMMENDED PROCESS (Cont'd)

- Firm contracts with service provider:
 - [see "Conclusions" below]
- Report/billing by service provider
- General statistics, without PI, or
 - Minimal PI for verification purposes and with consent of employees

Scenario #2

BC, Alberta and Saskatchewan operations with HR records centralized in Alberta.

You are the Human Resources Manager for a large heavy equipment rental outlet in British Columbia with a head office in Alberta and a further outlet in Saskatchewan. The entire business is operated through Tough Equipment Ltd., a federally incorporated company. The management at head office in Alberta wish to have personnel information for all employees consolidated in a centralized database which will be located in Alberta. The information in the database would then be accessible to local management of the outlets in British Columbia and Saskatchewan, as well as to head office management in order to best utilize human resources information to place employees as optimally as possible and to identify employees who should be groomed for management positions in the various outlets. The Human Resources Manager from the Saskatchewan outlet says that there are no privacy law issues involved because the information is all staying within the one corporation and because privacy laws only apply to employees of federally regulated entities such as airlines and banks, not to an equipment rental company, even if it operates in more than one province. You wonder if the federal incorporation makes your company federally regulated.

Questions arising:

- Is the Saskatchewan Human Resources Manager correct?
- You believe no consent is required to transfer this employee information to the head office in Alberta and the only obligation is to notify the employees ahead of time that this will occur. Your Alberta Director of Human Resources thinks consent is required. Who is correct?
- The head office systems technician says that since the employees are all employed by the one corporation, the only security required for the database are firewalls etc. that will prevent someone from outside the corporation obtaining access to the data. You are uncertain about this. Are you right to be concerned?

Scenario #2

FEDERAL JURISDICTION OVER EMPLOYEE PI

- PIPEDA only applies to federally regulated employers
- Not federally regulated because federally incorporated
- Only certain industries are federally regulated
 - e.g. banks, telecommunications, interprovincial transport, aeronautics
- This scenario
 - employer subject to laws of each province

11

Scenario #2

PROVINCIAL PRIVACY LAWS

- BC and Alberta both have privacy legislation
 - Covers collection, use or disclosure of PI in either province
- All PI in centralized database in Alberta subject to Alberta PIPA

12

Scenario #2

PROVINCIAL PRIVACY LAWS (Cont'd)

- Employer is one "organization"
 - Collection and use within organization must be reasonable
 - "Use" may include disclosure within the organization
 - Such disclosure OK if reasonable > consent not required
 - Storage in employer's centralized database OK without consent

13

Scenario #2

EMPLOYEE PERSONAL INFORMATION

- Special definition in BC and Alberta PIPA
 - Solely for the purposes, and
 - Reasonably required to establish, manage or terminate the employment relationship
- Greater scope for collection, use and disclosure of employee PI without consent
 - But, requires prior notice of purpose

14

Scenario #2

SECURITY OF THE DATABASE

- Make “reasonable security arrangements”
 - Prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks
- Use within the organization must be reasonable
- Employee PI accessible only as reasonably necessary

15

Scenario #2

RECOMMENDED PROCESS

- Follow Alberta/BC standards
- Notice of HR records being centralized in Alberta, to
 - Prospective employees on application for employment
 - Current employees at time of hiring
- Establish protocol for security of PI
- Limit access to PI
- Educate those with access to PI

16

Scenario #3

Workplace injury data from BC, Alberta, Ontario, Quebec and U.S. subsidiaries centralized in German parent company for use by outside consultant in Germany.

You are the Chief Privacy Officer for a furniture manufacturer and retail company with a head office in Germany and subsidiaries in various U.S. states and Canadian provinces, including British Columbia, Alberta, Quebec and Ontario. The Director of Safety at the head office wishes to hire an outside consulting firm to assist the organization and its subsidiaries in better managing work-related injuries and the costs associated with same. Accordingly, the Director of Safety is asking all Plant Managers to input information regarding work-related injuries into a centralized database located in Germany and to update the database regularly with information such as number of days employee is absent, diagnosis, expected return date to work, etc. The outside consultants (also located in Germany) would then access the database in order to monitor situations on an on-going basis and to provide advice and support where appropriate.

Questions arising:

- The Plant Manager at the Alberta subsidiary sees no problem with this arrangement and says that so long as employees are notified that this is occurring, no consent is necessary. Is this correct?
- The Plant Manager in B.C. is in favour of this program but is concerned that it may not be permissible to disclose the employees' diagnosis to an outside organization. Is he right to be concerned?
- The U.S. Plant Managers are in favour of the program and do not see why any consent or notification of employees would be required.

NATURE OF PERSONAL INFORMATION

- **BC and Alberta:** Should be “employee personal information”
 - Except: diagnosis information may not be “reasonably required”

- **Québec:** No special provisions for employee personal information
 - Must be “necessary” and objects identified in advance

NATURE OF PERSONAL INFORMATION (Cont'd)

- **Ontario:** No statutory restrictions except for “personal health information”
 - Applies to “health information custodian”
 - May be collective agreement and common law restrictions on confidentiality of PI

NATURE OF PERSONAL INFORMATION (Cont'd)

- **U.S.:** No statutory regime
 - May be industry or self regulatory regimes

- **Germany:** European Union Directive and national legislation protecting PI

WHAT IS THE "ORGANIZATION"?

- **BC and Alberta:** Each subsidiary an "organization"
- **Québec:** Each subsidiary a separate "enterprise"
- **Germany:** Parent and consultant both bound by EU Directive and national law

- Contrast with Scenario #2

NOTICE / CONSENT

- **BC and Alberta:** Except for diagnosis, reasonable to collect, use and disclose
 - *Prior* notice and statement of purpose
- **Québec:** Free and informed consent, preferably in writing
 - Consent to disclose to parent *and* consultant
 - Use and disclosure consistent with consent

NOTICE / CONSENT (Cont'd)

- **Ontario:** Express or implied consent generally required
 - For collection, use or disclosure
 - of "personal health information"
 - by "health information custodian"

c

NOTICE / CONSENT (Cont'd)

- **U.S.:** No statutory regime
 - May be industry or self regulatory regimes

- **Germany:** Collection, use and disclosure:
 - Fair and lawful, for justified interests, with unambiguous consent

RECOMMENDED PROCESS

- Consider all the circumstances and risks
 - Consent from all employees or just Québec?
 - Notice to all without seeking consent?
 - Consult union on consent vs. notice
- Contractual commitments of parent and consultant
- Education and risk management
- Security and access to database

Scenario #4

U.S. based services to BC government from offices in Vancouver and Seattle.

You own a small business (incorporated in Washington State and operating in both Seattle and Vancouver) which provides media training and public speaking skills development. The Ministry of Tourism wishes to hire your organization to provide training and coaching services to some of the Ministry employees. In order to provide these services, you will need to obtain and keep on file information about each of the employees to be coached, their educational and employment background, their position and responsibilities, their previous experiences with public speaking and the media, etc. and you will also need to take and retain notes regarding your training sessions with them and their performance throughout.

You are generally familiar with *PIPA* and have a privacy policy in place. You are surprised when the Personnel Manager from the Ministry states that the *Freedom of Information and Protection of Privacy Act* (“*FOIPPA*”) applies and that you must be compliant with same. You are even more surprised when the Director of Personnel indicates that it will be a problem under *FOIPPA* for you to work on this project both from your British Columbia and Seattle offices and for you to store any information relating to your services in your main computer at the Seattle office.

Questions arising:

- Why is the Ministry Personnel Manager suggesting that *FOIPPA* applies when, as far as you know, your organization is regulated by *PIPA*?
- If *FOIPPA* does apply, what does this mean for your organization in this situation?
- Can the notes from the training sessions be taken to or kept in Seattle?

APPLICABLE LEGISLATION

- BC government subject to FOIPPA
 - “public body”, its employees, officers and directors, subject to FOIPPA
 - PI provisions in Part 3
 - Collection, use, disclosure, storage and access, and retention of PI
 - Separate provisions for disclosure inside and outside Canada

APPLICABLE LEGISLATION (Cont'd)

- Service provider and its employees:
 - Subject to FOIPPA
 - PIPA not applicable to PI from this contract
 - Otherwise covered by PIPA

PUBLIC BODY COLLECTION AND CUSTODY

- Collection if necessary for operating program or activity
- Notice of purpose, legal authority and name of privacy officer
- Reasonable security arrangements
- PI in its custody or control:
 - Store and access in Canada only, unless consent or allowed by 30.1(b)

PUBLIC BODY USE AND DISCLOSURE

- Use:
 - For purpose or consistent purpose, OR
 - Possibly, with detailed consent in writing

- Disclose *inside* Canada
 - For purpose or consistent purpose, OR
 - If necessary for service provider to perform its contract

USE AND DISCLOSURE TO SERVICE PROVIDER

- Disclose *outside* Canada
 - If necessary for service provider to perform its contract, and
 - Normally disclosed inside Canada but service provider temporarily outside Canada

- Contract for compliance with FOIPPA

RECOMMENDATIONS FOR SERVICE PROVIDER

- Written consent from employees
- Keep all PI in Canada
- Only store or access PI outside Canada with consent
- Educate employees re FOIPPA compliance
- Cannot apply “employee personal information” provisions of PIPA

CONCLUSIONS

- Managing parent company demands / expectations
 - Know your privacy obligations
 - Pitch the privacy culture
 - Turn necessity into virtue
 - An employer's approach to PI can be recruitment/retention tool
 - Education and risk management

33

CONCLUSIONS (Cont'd)

- Managing employee PI across borders
 - Transparency for employees and their PI
 - Comprehensive and regular reminders
 - Written and signed consents when practical
 - IT security and protocols
 - including portable data issues
 - Consistency throughout the corporate family
 - Follow the most stringent requirement when practical

34

CONCLUSIONS (Cont'd)

- Managing service providers
 - Make privacy experience a selection criterion
 - Establish a comprehensive contract
 - Cover all applicable privacy obligations
 - Make privacy compliance a material term
 - Prohibit unauthorized/unnecessary disclosure
 - Regular reporting on privacy compliance
 - Security obligations and breach protocol
 - Privacy audits
 - Indemnities for privacy breaches

35

SOURCES

BC Privacy Commissioner

<http://www.oipcbc.org/>

FOIPPA [http://www.oipcbc.org/legislation/OLD_ACTS/FIPPA-ACT\(21Nov2006\).pdf](http://www.oipcbc.org/legislation/OLD_ACTS/FIPPA-ACT(21Nov2006).pdf)

PIPA [http://www.oipcbc.org/legislation/PIPA/PIPA\(2006\).pdf](http://www.oipcbc.org/legislation/PIPA/PIPA(2006).pdf)

20th Century Fox decision <http://www.oipcbc.org/PIPAOrders/2006/OrderP06-04.pdf>

Alberta Privacy Commissioner

<http://www.oipc.ab.ca/home/>

Federal Privacy Commissioner

http://www.privcom.gc.ca/index_e.asp

PIPEDA http://www.privcom.gc.ca/legislation/02_06_01_e.asp

CIBC outsourcing case http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp

PI shared with U.S. parent http://privcom.gc.ca/cf-dc/2006/333_20060511_e.asp

MANAGING EMPLOYEE PERSONAL INFORMATION: CROSS BORDER AND OUTSOURCING CHALLENGES

Tamara L. Hunter
Davis LLP
Barristers & Solicitors
2800 Park Place, 666 Burrard Street
Vancouver, British Columbia V6C 2Z7

Direct: (604) 643-2952
Fax: (604) 605-3712

Email: tamara_hunter@davis.ca

Earl G. Phillips
McCarthy Tétrault LLP
Barristers & Solicitors
Suite 1300, 777 Dunsmuir Street
Vancouver, British Columbia V7Y 1K2

Direct: (604) 643-7975
Fax: (604) 605-5275

Email: ephillips@mccarthy.ca

DAVIS | LEGAL ADVISORS
LLP | SINCE 1892

McCarthy
Tétrault

MCCARTHY.CA