OSLER

Data Management in Franchise Systems

Evan Thomas - Osler Hoskin & Harcourt LLP
Dan Vukovich – M&M Meat Shops
CFA Franchise Law Day – January 28, 2016

Overview

- Like other businesses, franchise systems are making increasingly sophisticated use of customer, financial, operational and other data.

- Collecting, using and protecting this data to successfully advance the system's business objectives requires close co-operation between franchisors and franchisee.

- Focus of this presentation is on how to take advantage of the new data environment while managing the associated legal challenges.

OSLER

OSLER

Objectives

- Understand legal landscape associated with the business opportunities of “Big Data”.
- How to mitigate common legal risks under privacy legislation for franchisors.
- How to address collection and use of data by franchisees in the franchise agreement.
- How to respond to incidents involving the loss or misuse of sensitive data.

OSLER

What is the Opportunity?

- Businesses – including franchise systems – capturing increasing volumes of:
  - Consumer data
  - Financial data
  - Operational data
- Data analytics ("Big Data") increasingly used for critical business decisions in franchise systems:
  - Marketing
  - Site selection
  - Product planning
  - Process improvement

OSLER

What are the Risks?

- Big Data magnifies the following risks:
  - Loss or exposure of data due to technical or human error.
  - Unauthorised access to data by malicious third parties using technical or other means to avoid protections.
  - Unauthorised use by employees/franchisees/others of data to which they have access.
  - Objections by individuals (or regulators) to how personal data is used.
  - Commercial disputes with franchisees and others over the value of data.

What are the Consequences?

- Brand/reputation damage
  - Media are quick to report on major (and even minor) incidents involving loss or misuse of data
  - Consumers becoming increasingly sensitive to how their personal information is used

- Civil liability
  - Increasing recognition of privacy torts by courts
  - Consumer privacy class actions
  - Claims by third parties

- Regulatory Investigations/Liability
  - Privacy regulators increasingly active and willing to impose penalties for non-compliance

OSLER

OSLER

Why are Franchise Systems Different?

- Organizational structure
  - May amplify risks and makes policy compliance more challenging
- Geographic reach
  - Tend to operate in multiple jurisdictions
- Brand
  - Key asset for both franchisor and franchisees
- Each of these factors tends to make managing data practically and legally more complex

Franchise-Specific Issues

- Practical issues:
  - How are franchisees' IT systems kept up-to-date and secure?
  - How does data flow between franchisor and franchisee?
  - How are franchisees' employees trained on privacy compliance?
- Legal issues:
  - Which party is collecting information for purpose of privacy legislation?
  - Which party "owns" the information collected in the course of executing the system?
  - Which party is responsible for maintaining IT systems and technical data security measures?
  - Which jurisdiction's (or jurisdictions') privacy legislation may apply when the franchisor and franchisee are in different jurisdictions?
  - What are the franchisor's rights/powers in the event of an incident involving a franchisee?

OSLER

Legal Landscape

- Managing data in franchise systems takes place in context of:
  - Increasing obligations under privacy law
  - Legal uncertainty around data “ownership”
  - Complex web of vendor agreements
  - Potential directors and officers liability
  - Gaps in legacy franchise agreements

OSLER

OSLER

Increasing Privacy Obligations

- Like other Canadian businesses, franchisors and franchisees may be subject to federal or provincial privacy protection legislation.
- Privacy regulators becoming increasingly active and are armed with more extensive powers.
- Growing judicial recognition of new common law "privacy torts" (intrusion upon seclusion, publicity given to private life) exposing defendants to civil liability.
- Courts increasingly certifying privacy class actions relating to privacy incidents affect large groups of people.

Increasing Privacy Obligations – Breach Notification

- Whether to impose a duty to notify individuals affected by a data breach has been contentious policy issue for many years.
- Policy direction moving rapidly towards mandatory breach notification.
- Alberta legislation requires notification to the Alberta privacy commissioner where there is a "real risk of significant harm" to individuals.
    - Orders have been made against organizations outside of Alberta where Albertans affected.
- *Digital Privacy Act* amended *PIPEDA* to among other things add a new breach reporting, notification and record-keeping requirement (not yet in force).
- Once in force, organizations subject to PIPEDA must to report and notify affected individuals where there is a "real risk of significant harm".

OSLER

OSLER

Uncertainty Around Data Ownership

- Data increasingly viewed as an asset to be monetized, either through analytics to improve the business or by licensing the data.
- Whether “data” can be owned in Canadian law is a complex legal question.
- Protection of commercial value of data usually accomplished by contract and law of confidential information.
- Trade secret and copyright law may also apply.

OSLER

Complex Web of Vendor Agreements

- Many franchise systems outsource business functions/processes that involve collection, storage and use of data.
- Franchise systems may also obtain data from third parties (demographic data, survey data, consumer profiles, etc.)
- Data may flow to and from variety of third parties:
  - IT service providers
  - Marketing agencies
  - Printers/mail houses
  - Consultants
- Outsourcing agreements may not address risks associated with sharing data with third parties.
  - Organizations retain responsibility for privacy compliance in respect of the personal information transferred to the service provider.
- Agreements under which data is acquired from other parties may impose restrictions and other obligations on franchisor with respect to how it may use the data.

OSLER

Potential Directors and Officers Liability

- Not exclusively a public company issue; statutory duty of care in most corporate statutes is not limited to the corporation or its shareholders.
- In theory, directors and officers may be liable to variety of stakeholders, if they have failed in their duty of care.
- Increasingly common for directors and senior executives to request audits or other assurances regarding security of the company's data and compliance with privacy laws.

Gaps in Franchise Agreements

- Many “legacy” franchise agreements are entirely, or mostly, silent on:
  - Compliance with privacy law
  - “Ownership” of customer and other information
  - Information technology and data security issues

- These gaps can increase risk of franchise disputes regarding which party:
  - is responsible for privacy law compliance
  - can use customer information and other data acquired or generated in the course of operating the system, and how
  - receives the benefit of monetizing data streams
  - is responsible for maintain technology systems/securing data

OSLER

Addressing the Risks: Privacy & Data Governance

- Do you know:
  - what data is being collected?
  - what type of data is it (personal, financial, operational)?
  - from whom is it being collected?
  - have the suppliers of the data been informed of and/or consented to how it is being used?
  - why is it being collected or why was it collected?
  - where your data is?
  - what technical and other measures have been taken to protect it?
  - who has access to it?
  - how data is being used by the franchise system?
  - how long the data will be retained?
  - whether the data is being shared with third parties and for what purpose?
  - whether the data is subject to any form of licensing agreement?
  - is there still a valid business purpose in collecting/retaining it?
  - how the data will be disposed of and when?

- Absent an understanding of the data and data flows within the franchise system, very difficult to address all of the risks associated with data.

- Best practice: A comprehensive privacy/data governance framework for the organization.

OSLER

Privacy/Data Governance Framework

- Typical elements:
  - Roles and responsibilities
  - Status and issue reporting mechanisms
  - Policy governance
  - Operational governance
    - New uses of data
    - Process changes
    - Records management
    - Data inventory
    - Risk management
    - Training
    - Incident response
    - Compliance monitoring
    - Vendor management

OSLER

Privacy Compliance

- Compliance with applicable privacy law is one of the primary objectives of an effective privacy and data governance framework.

- Existence of framework also assists in demonstrating organizational diligence in the event of non-compliance.

- A privacy and data governance framework in a franchise system should address roles/responsibilities, reporting and governance as they pertain to franchisees as well as franchisors.

OSLER

Vendor Agreements

- Review agreements to determine whether they address the system's interests and/or are consistent with governance framework with respect to:
  - Confidentiality of franchisor/franchisee data
  - Limits on use vendor may make of the franchisor/franchisees' data
  - Limits on use franchisors/franchisees may make of third party's data
  - Retention of data by vendor or franchisor/franchisee after relationship ends
  - Managing data in compliance with applicable privacy law
  - Co-operation in the event of a data security incident
  - Allocation of risk of civil or regulatory liability (indemnities, limitation of liability clauses)

OSLER

OSLER

Directors and Officers Liability

- Specific obligations of directors/officers with respect to data security/privacy compliance will depend on their position and knowledge.
- Increasingly common for directors and senior executives to request audits or other assurances regarding security of the company's data and compliance with privacy laws.
- Once aware of any issues, directors/officers may be obligated to take appropriate steps to ensure issues addressed.
- Existence of privacy/data governance model will help directors/officers in fulfilling their obligations.

OSLER

Franchise Agreements

- Review franchise agreements in context of governance framework to identify any gaps with respect to collection, use, storage, sharing and retention of data, particularly personal information.
- Update franchise agreements as franchises added/existing agreements are renewed.
- Determine if gaps in long-term legacy franchise agreements can be addressed through:
  - Updates to operating manual
  - Ancillary agreements
- Keep in mind potential disclosure issues under applicable franchise law.

Data Security Incidents (Data Breach)

- A data security incident (data breach) occurs when information is copied, transmitted, viewed, stolen or used by someone without authority to do so:
  - Computer/network intrusion
  - Loss of data
  - Technical error
  - Unauthorized access/use

- Every organization should have a pre-existing plan for responding to such an incident, either as part of a privacy/data governance framework or otherwise.

- Having an existing plan may mitigate the risk/cost of an incident and helps demonstrate the organization's due diligence

OSLER

OSLER

Response Plan

- Basic elements:
  - Containment
  - Investigation
  - Consultation with regulators (if required/advisable)
  - Notification of affected individuals (if required/advisable)

- Plan may also address the participants in the response (IT, Human Resources, Legal, etc.) and identify who has the lead, which may depend on the nature of the incident.

Response Plans in Franchise Systems

- Major incidents involving franchisees will practically (if not legally) require involvement of franchisor.

- Best Practice:
  - Franchise agreements and/or manuals should address how data breaches involving franchisees will be managed and require the franchisee to cooperate with the franchisor.

OSLER

Data Security Incident Investigations

- Common questions following a data security incident:
  - How did it happen (lost USB, software vulnerability)?
  - Why did it happen (human error, malicious attack)?
  - What information was involved?
  - Was the information exposed?
  - To whom does the information relate, if anyone?
  - What was accessed (SINs, CC numbers)?
  - When did it happen and how long, if applicable?
  - Who was involved (employee, unknown attacker, vendor)?

OSLER

Investigations - Legal Considerations

- In-house or outside counsel may require this information to provide advice regarding:
  - Whether the organization is obligated to report the incident to a regulator and if so, how
  - Whether the organization is obligated to notify affected parties and if so, how
  - Whether the organization has potential exposure to fines or other penalties
  - Whether the organization has potential exposure to civil claims by affected parties
  - Whether the organization has claims against the persons at fault for the incident

OSLER

Investigations – Non-Legal Considerations

- Information may also be required for other purposes:
  - Remedying technical issues
  - Improving technical data security practices
  - Taking personnel action
  - Informing executives/board of directors
- The results of the investigation may be communicated to a variety of stakeholders
  - IT staff
  - Executives/directors
  - Legal counsel
  - Regulators
  - Customers
  - Vendors
- Investigations may require the involvement of third parties (data suppliers and vendors)

OSLER

OSLER

Investigations – Franchise Context

- Franchisees are a stakeholder group not found in other organizations.
- A data security incident may directly or indirectly franchisees.
- Franchisees may be required to participate in any investigation.
- Franchisees may in any event be interested in the outcome of the investigation.

OSLER

Privilege Considerations

- Whether legal privilege attaches to the communications and findings of an incident investigation may depend on who conducts it, how it is conducted and its purpose.

- Confidentiality is an essential element of solicitor-client privilege; absent common interest or some other special circumstance, including third parties in privileged communications generally negates the privilege.

- Whatever the approach, important to remind participants in the investigation to stick to the facts and to avoid personal opinions and theories.

Best Practices – Investigations

- Employees should:
  - Provide factual information to counsel
  - Avoid speculation and personal opinion
  - Limit the dissemination of the information
- Outside experts should:
  - Be engaged to gather and analyze information for purpose of legal advice
  - Address reports and updates to counsel
- Counsel should:
  - Avoid providing legal opinions or advice in the presence of the expert

OSLER

OSLER

Best Practices – Third Party Vendors

- Where co-operation/involvement of third party vendors is necessary, communications with vendor (or within vendor's organization) may not be subject to privilege.
- If possible, include specific language in agreements providing:
  - Parties have common interest in any investigation
  - Vendors will co-operate fully
  - Vendors will maintain confidentiality
- If not possible, when incident occurs, attempt to obtain such an agreement.
- Such terms can strengthen argument parties have common interest and do not intend to waive privilege.

Best Practices - Franchisees

- Similar considerations to third parties.
- Co-operation from franchisee may be required but privilege will not necessarily attach to communications with the franchisee.
- If the franchise agreement or an agreement made at outset of the investigation establishes a common interest, co-operation and confidentiality, privilege argument strengthened.

OSLER

Conclusion

- Tremendous business opportunities of Big Data can be undermined by avoidable incidents.

- In addition to mitigating risk, introducing privacy/data governance is a potential business advantage, by requiring system to critically evaluate what data is required to execute and improve the system to the mutual benefit of franchisors and franchisees.

OSLER