EXPLORING THE INTERSECTION OF PRIVACY LAW AND FRANCHISE LAW
Considerations for Franchisors and Franchisees Alike in Navigating Privacy Issues in 2020 and Beyond

By: Christopher Oates (Gowling WLG), Adrienne Boudreau (Sotos LLP), and Jason Brisebois (Sotos LLP)

1. Introduction and Sources of Franchise Privacy Obligations[1]

Canadian privacy legislation at both the federal and provincial levels imposes compliance obligations on franchisors and franchisees, alike. This paper describes core considerations for compliance with Canadian privacy law, and applies them to the franchise context, discussing commonly encountered issues such as who exercises control over the data, the role of franchise agreements in addressing privacy issues, service provider agreements, breach response and Canada's Anti-spam Legislation.

The applicable legislation will depend on the jurisdiction in which the organization operates, the nature of its business, and on the manner in which it collects, uses and discloses personal information. Three provinces, British Columbia[2], Alberta[3], and Quebec[4], have in place private sector privacy legislation that will apply to organizations within those provinces, or that process the personal information of individuals from those provinces. Federally, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), applies to the collection, use, and disclosure of personal information in the course of commercial activities.[5] PIPEDA will apply to the collection, use or disclosure of personal information in the remaining provinces and territories, as well as international and interprovincial transfers of personal information. As a result of this overlapping legislation, a national franchise system will be subject to all four laws.[6]

These four laws represent the primary private-sector privacy laws in Canada. Layered on these are additional legislative regimes that while not privacy laws per se, do create requirements for the collection and processing of personal information. Among these are Canada's Anti-Spam Law (CASL)[7], which creates an onerous regime surrounding email and other forms of electronic

[1] The authors would like to acknowledge their appreciation for all of the efforts of Dominic Mochrie, Osler, Hoskin & Harcourt LLP, and Anna Thompson-Amadei, Sotos LLP, in respect of this paper.
[2] *Personal Information Protection Act*, SBC 2003, c 63 [*BCPIPA*].
[3] *Personal Information Protection Act*, SA 2003, c P-6.5 [*ABPIPA*].
[4] *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 [Quebec Act].
[5] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].
[6] At the time this article was written, Ontario had recently concluded a consultation on strengthening privacy protection within the province. This may culminate in the introduction of an Ontario private sector privacy law, however, no proposed legislation has been published as yet. Online: https://www.ontario.ca/page/consultation-strengthening-privacy-protections-ontario.
Separately, Quebec has proposed a major reform to its privacy legislation in the form of Bill 64, which among many other things, will if adopted raise the stakes by introducing penalties of up to $25,000,000, or an amount corresponding to 4% of worldwide turnover for the preceding fiscal year. Online: http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html.
[7] *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23 [CASL].

messaging, and the Unsolicited Telecommunications Rules under the Telecommunications Act[8], which govern telemarketing.

While this paper will primarily focus on the application of private sector privacy laws in a franchisor/franchisee context, it is important to note that additional laws may apply to the activities of franchise organizations in particular sectors, or engaging in particular activities. For example, public sector privacy legislation, including its "access to information" obligations, may become applicable in a context where a franchise location is operated in association with a public sector entity, such as a university or hospital. Likewise, many provinces have health sector specific legislation that may be implicated in cases where personal health information is collected or processed. These public sector and health sector laws are beyond the scope of this paper, but must be considered by organizations doing business with entities subject to them. Canada's private sector privacy laws are based on fair information principles that, among other things and subject to stated exceptions, require organizations to be responsible or accountable for information under their control[9], require informed consent to the collection, use, and disclosure of personal information[10], and that obligate organizations to provide appropriate security for personal information[11], including in cases where that information is transferred to a third party for processing.

Personal Information

Before considering the obligations under Canadian privacy law in more depth, it is worth addressing the meaning of "personal information". Information will be "personal information" where the information is about an "identifiable" individual. Key to the concept of personal information is that the individual must be identifiable; it is not necessary that they be directly identified by the information for the privacy laws to apply.

The concept of "personal information" has been given a broad interpretation by the federal and provincial privacy commissioners, as well as by the courts, with the test that is usually applied considering whether there is a "serious possibility" that an individual could be identified using that information, either alone or when it is combined with other information.[12] As a result of this, information that may at a glance not be thought of as "personal information" may amount to personal information if the circumstances are such that it could be identified. For example, the Federal Privacy Commissioner has ruled that IP addresses can amount to personal information[13], and has indicated that information collected and used for online behavioural tracking and advertising will generally be considered personal information by the Commissioner[14].

---

[8] *Telecommunications Act*, SC 1993, c 38

[9] See *PIPEDA*, *supra* note 5 at Schedule 1, s 4.1, *BCPIPA*, *supra* note 2 at s 4, *ABPIPA*, *supra* note 3 at s 5, and Quebec Act, *supra* note 4 at s 1.

[10] See *PIPEDA*, *supra* note 5 at Schedule 1, s 4.3, *BCPIPA*, *supra* note 2 at s 6, *ABPIPA*, *supra* note 3 at s 7, and Quebec Act, *supra* note 4 at s 14.

[11] See *PIPEDA*, *supra* note 5 at Schedule 1, s 4.7, *BCPIPA*, *supra* note 2 at s 34, *ABPIPA*, *supra* note 3 at s 34, and Quebec Act, *supra* note 4 at s 10.

[12] *Gordon v Canada (Health),* 2008 FC 258 (CanLII).

[13] PIPEDA Report of Findings #2009-010.

[14] Office of the Privacy Commissioner of Canada, "Policy position on online behavioural advertising", (Ottawa: OPC, December 2015) online: <https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/bg_ba_1206/>

Consent

To collect, use, or disclose personal information, Canada's private sector privacy laws require the informed consent of the affected individual. For consent to be valid, it must be reasonable to believe that the individual will understand the nature, purpose, and consequences of what they are consenting to.[15] Consent must be for disclosed -and understandable- purposes. Broad, open-ended consent that could conceivably allow any use or disclosure of personal information that an organization may deem desirable in the future is not valid. As a result, organizations must consider how information will be used and disclosed prior to collecting it.

To guide organizations on this principle, the federal office of the Privacy Commissioner of Canada ("OPC"), and the Commissioners in the provinces of British Columbia and Alberta have jointly published Guidelines for Obtaining Meaningful Consent.[16] The Guidelines focus on the experience and understanding of the individual providing consent, and require great transparency over the information collected and how it will be used and disclosed, paired with great clarity, simplicity, and understandability. This creates an increasing challenge, in particular in online contexts where the manner in which potentially identifiable information is collected and used is not simple, but to obtain valid consent, it will nevertheless need to be presented in a way that the average individual will be able to understand. Plain language is encouraged: overly technical or legalistic descriptions of collections and uses of personal information are not likely to be viewed by the Commissioners as amounting to valid consent, even in an online context where such collection and use is inherently technical and difficult for the average person to understand.

To square this circle, the Commissioners recommend emphasising what they consider the key elements of informed consent:

1. **What personal information is being collected?** In order to understand what they are agreeing to, individuals must be clearly told what information is collected.
2. **Who is that information shared with?** The information shared with third parties, and the classes of third parties involved, must be clearly explained. In a franchisor/franchisee context, particular consideration should be given to the manner in which the franchisor and franchisee exchange personal information. If information is disclosed to a third party for their own use (as opposed to a third party processing the information for the entity that disclosed it), that disclosure should be given particular emphasis.
3. **For what purposes is the information collected, used, or disclosed?** All purposes for which personal information is collected, used, and disclosed must be clearly stated in a manner that avoids vague terminology. Organizations should pay particular attention to uses or disclosures of information that are not obvious or intuitive. For example, a consumer using a debit or credit card to make a purchase understands that information associated with their card is processed to effect payment. Secondary processing of consumer information, for example, tracking purchase habits for the purpose of targeting marketing, would not be intuitive and must be clearly explained, along with any choices the individual has to opt out. Consent to the collection, use or disclosure of personal

[15] *PIPEDA*, *supra* note 5 at s 6.1.
[16] Office of the Privacy Commissioner of Canada, "Guidelines for Obtaining Meaningful Consent", (Ottawa: OPC, May 2018) online at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

information cannot be a condition of service unless the collection, use, or disclosure is necessary to provide that service. For example, an individual must not be required to agree to marketing using their personal information as a condition of receiving a product or service.

4. **Is there any risk of harm?** Individuals must be informed of any residual risks of harm that remain despite any mitigation measures undertaken by the organization.

As a practical matter, both franchisors and franchisees should consider what personal information they collect, how it is collected, how it is used and disclosed, and whether each of those activities is carried out by the franchisor, the franchisee or both. Only with a clear understanding of those practices will it be possible to address how to obtain consent to the collection and processing of the personal information.

Control and Accountability

In a franchisor/franchisee relationship, the concept of control and accountability over personal information will create obligations that apply to both parties, in particular where one entity collects personal information, then provides it to the other for processing and use. The private sector privacy laws specify that organizations are responsible for personal information within their control. "Control" is a broad concept that considers an organization's authority to determine how personal information is collected, used, or disclosed, for how long it is retained, and how it is disposed of. Where an organization has control over personal information, it remains responsible for that information even when the information is in the hands of a third-party processor. For example, PIPEDA specifies that organizations transferring personal information for processing must use "contractual means" to ensure that the information remains appropriately protected.[17] Further, as the organization with control remains accountable for the information in the hands of their service provider, they should undertake due diligence efforts, commensurate with the sensitivity of the information being processed, to ensure that the information is appropriately used, protected and ultimately deleted.

Where personal information is transferred from a franchisee to a franchisor, or vice versa, the entities should address the ownership and control of the personal information in the franchise agreement (or other ancillary agreements) between them, or in the franchisor's operations manual, a matter we address further in the next section. Similarly, where either a franchisor or franchisee engages a third party service provider to process personal information, they must use an appropriate form of data protection agreement to ensure the personal information remains appropriately protected, a matter addressed in more detail in section 3.

Two recent decisions of the OPC and the Office of the Information and Privacy Commissioner for British Columbia (OIPC BC) have greatly increased the responsibilities of organizations that are disclosing personal information to a third party, or receiving information from a third party.

In a decision released in April 2019, the OPC and OIPC BC released findings into the manner in which Facebook allowed third-party applications to obtain personal information from its users.[18] Facebook allowed third-party applications (for example, personality quizzes and games) to obtain

[17] *PIPEDA*, *supra* note 5 at Schedule 1, s 4.1.
[18] PIPEDA Report of Findings #2019-002.

the "consent" of individuals for Facebook to disclose their personal information to the application publisher. In disclosing such information, Facebook sought to take a threefold approach to establish consent: i) all users were required to agree to the Facebook Data Use Policy, which explained how applications may obtain permission to use personal information; ii) when a user installed an application, they were presented with a dialog box explaining what information the application received, and iii) the application publisher was required in its contract with Facebook to explain its privacy practices in its own privacy policy.

However, the Commissioners expected Facebook to take a much more direct role in securing consent to disclose personal information to application developers. In particular, they wanted Facebook to review the privacy communications and policies of the application developers to verify their content before disclosing personal information to them. Considering that there are tens of millions of applications on Facebook, the amount of resources required to assess the compliance of the privacy policies of each one, which may be subject to differing requirements depending on the jurisdiction in which a particular Facebook user interacting with the App resides, would be an onerous undertaking.

In November 2019, the OPC and OIPC BC released findings in respect of AggregateIQ, a company that provided data processing and targeted advertising services to political campaigns in Canada, the United States and United Kingdom.[19] AggregateIQ received personal information from its clients, then used that information to target political information to the individuals. The Commissioners reviewed the manner in which AggregateIQ processed this information, and contrasted it with the consent obtained by AggregateIQ's clients. In instances where the processing performed by AggregateIQ was outside the scope of the consent obtained by the client, or in cases where the client had not obtained consent, the Commissioners held that AggregateIQ was in violation of PIPEDA and BC PIPA. The Commissioners indicated that they expected data processors to undertake 'reasonable' measures to ensure that their clients obtained meaningful consent to the processing of personal information the client requested. These measures were to include contractual measures (for example, warranties that adequate consent had been obtained), and the data processor reviewing the consent language used by their client and assessing its adequacy with Canadian privacy law.

While neither of these decisions are in the franchise context, franchisors or franchisees who are faced with an investigation by the OPC or OIPC BC can expect to face a similar position from these Commissioners. For example, a franchisee receiving personal information from a franchisor to aid in its marketing efforts would be expected to be able to demonstrate that the franchisor obtained adequate consent to allow the franchisee to use the information in this manner. A franchisor receiving identifiable sales data from a franchisee would be expected to review the consent practices of the franchisee to ensure that adequate consent had been obtained to allow the franchisor to process the information.

The same consideration would apply to a context where either a franchisor or franchisee receives personal information from the operator of a food delivery app, such as DoorDash or Foodora, or from another co-promotional partner.[20] In such a context, the parties must first establish what, if

[19] PIPEDA Report of Findings #2019-004.

[20] That is, an entity contrasted with a true service provider who may process personal information, but does so only at the instruction and under the control of their client, and typically, does not have consumer visibility.

any, identifiable data is exchanged, the purposes for which the information would be used, and the role of each party in establishing consent to such an exchange and use of information.

To take the relatively simple case of a food app operator agreeing to request email marketing consent for the franchisor, for example, on the application itself, the consent language used would need to comply with both the privacy laws, and with CASL (which is treated in more detail below). If the consent language was not compliant, there would be the potential for either the franchisor or the operator of a food delivery app, or both, to be found offside the privacy laws. For example, in using email addresses obtained from the operator of the app where the operator did not obtain adequate consent, the franchisor would be using personal information without appropriate consent. Likewise, in disclosing the personal information for a purpose where they had not established adequate consent, the app operator would be disclosing personal information without appropriate consent. The difficulty on this point is compounded where the disclosure and use of the information is not intuitive. A consumer can easily understand a request to send them commercial email about an identified franchise. Exchanges of information for the purposes of profiling or tailoring targeted advertising can be much less intuitive, and as a result, bear greater consideration from a consent perspective.

Practically, in entering such a relationship, franchisors, franchisees, and their third party vendors should consider what if any identifiable information is exchanged, whether the exchange is necessary for the services provided, and what the role of each party is in securing consent to and implementing individual choice in respect of that exchange. Having done so, the organizations should memorialize their arrangement via contract. However, reliance on contractual provisions alone will not be sufficient- it will be incumbent on each entity to review the consent language relied on and satisfy themselves of its validity.

Overall, recent decisions of the OPC and OIPC BC may make such negotiations, and ultimately the exchange of identifiable personal information, more difficult going forward. For a large franchise network where a franchisor is receiving personal information from many franchisees, the franchisor should keep in mind that a substantial majority of all of its franchisees will likely not have instituted a set of consent practices and guidelines relating to the data and personal information it collects from consumers and then distributes to the franchisor, including having established their own independent privacy policies. To address this, franchisors may consider including consistent standards on consent practices and privacy guidelines in the franchise agreement, an ancillary agreement, or in the franchisor's operations manual.

The franchisor will need to ensure that appropriate practices are implemented to ensure that the consent practices of its franchisees are consistent. The franchisor must be able to use any personal information it receives from the franchisees in a consistent manner, without implementing separate processing in respect of information received from each individual franchisee to account for differences in their privacy practices, an approach which may prove operationally cumbersome and unrealistic. Franchisors may consider taking a more hands-on approach with respect to franchisee privacy policies and consent practices- at least in so far as they result in the passing of personal information to the franchisor. If, for example, the franchisor is processing payments on behalf of the franchisees directly (or contracting a third party to do so), then the transfer of sensitive consumer payment information from the franchisee to franchisor for this purpose would likely be consented to by the consumer at the time of purchase. If this information is being used by the franchisor (or third parties) for additional purposes, however, then it is possible that the consumers

will not have adequately understood why they were providing their payment data to the franchisor, and therefore could not have provided informed consent regarding the usage of this data.

In considering what responsibilities exist with respect to the collection, transmission, and safeguarding of personal data, franchisors and franchisees alike must consider how the data they are collecting is used, disclosed, retained, and ultimately disposed of, as these factors will inform the extent of each party's control of this data, and ultimately, what each party's responsibilities are for the safeguarding of this data. Only after the organization has identified the manner in which it intends to collect personal information, and how such information will be used and disclosed, can it prepare appropriate consents to its practices, and an appropriate privacy policy that explains these practices in a complete and understandable manner that makes clear to the reader what entities access and use their personal information. As consent is required to collect, use and disclose personal information, this exercise must be undertaken prior to the collection of personal information. The organization should review its practices on a regular basis, at least annually, and should also conduct a review in cases where it intends to implement any changes to its existing practices. In cases where the organization determines that its consents and policies do not reflect its actual or intended practices, the consent language and policy will need to be updated, and the organization should cease processing information in a manner where it has not established adequate consent.

Ultimately, both the franchisor and the franchisees must have up-to-date privacy policies, and processes in place to obtain meaningful informed consent from the individuals whose information they collect, share and process.

2. Whose Data is it Anyway? Best Practices for Protecting Customer Data.

When considering which parties are responsible for protecting customer data, a crucial preliminary step is analyzing who owns the data – the franchisee, the franchisor, or a combination of the two parties. This determination will affect the responsibilities of the respective parties. Further, the matter may be more complicated when there are additional parties that may be providing or using the data, such as third party delivery aggregators, who claim that they own the data. The permutations are endless, and are outside the scope of this paper, which addresses ownership as between the franchisor and its franchisees.

Franchisees are often the first point of interaction that new and recurring customers will have with a particular franchise system, especially for brick-and-mortar businesses. Typically, customers will provide their personal information to the franchisee entity at the point of transaction. The customer may provide personal information to the franchisee for a variety of reasons, including as part of their purchase of goods or services, to enter into a contest, or in order to be enrolled in a newsletter or e-mail listserv. This franchisee may collect this information in accordance with any standards a franchise system has listed in their franchise agreement or operations manual, or pursuant to initiatives designed and implemented by the franchisee itself (assuming such initiatives are permitted pursuant to the relevant franchise agreement and operations manual). The relevant franchise agreement and operations manual may set out sample forms of consent or privacy practice; however even such a 'top-down' approach relies on the franchisee correctly implementing the forms. Of course, as is future discussed below, a franchisor must be mindful of exercising excessive control over the affairs of its franchisees, as such behaviour could render it being deemed a joint employer of the franchisees.

Keep in mind, however, that franchisors also often have access to franchisee systems, records, and databases, through centralized point-of-sale ("**POS**") hardware and software and other information technology systems. In addition to stipulating, directly or indirectly, that franchisees must collect certain personal information and other data from their customers, the franchisor may also require that this personal data be manually or automatically transmitted by the franchisee to the franchisor in order to enable the franchisor to analyze evolving business trends, carry out system-wide contests and promotions, or to review franchisee performance, among a wide variety of other uses.

As has already been explored above, private-sector privacy laws specify that entities are responsible for personal information within their control. Considering the high degree of interconnectivity that exists between the franchisee and the franchisor, often there will be overlapping control of customer data between the franchisee and the franchisor, and as a result, both parties must implement best practices and diligently police the use, transmission, and protection of data.

Key Considerations and Best Practices for Protecting Personal Data

Understand what Data the Business Requires and Plan Accordingly

Collecting, analysing, and acting upon consumer data is an increasingly critical tool that businesses are employing to improve their customer experience and to stay relative in hyper-competitive markets. It is imperative, however, that franchisors and franchisees alike collect and manage data in a manner that is reasonable and proportionate to their actual needs. Increasingly, businesses are practicing the concept of "data minimization", which Forbes described as the practice of "limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose."[21]

PIPEDA requires that businesses collect the least amount of personal informational necessary in order to meet the purpose of providing the product or service in question, or the purposes they have identified to the individuals, and to inform those individuals why this data is being collected.[22] Businesses can ask for information that goes beyond the purpose of providing the product or service; however, it must be clear to the customer that providing the information is optional. Businesses can also ask for consent to use the information for secondary purposes, such as marketing, if they indicate that it is optional.[23] By employing a data minimization strategy, franchisors and franchisees alike can ensure that they are not only complying with PIPEDA, but that they are limiting the data they are ultimately required to safeguard and manage to the lowest possible levels. In other words, the more data an organization has, the greater the potential harm in the aftermath of a data breach.

Worth noting is that the onset of COVID-19, a form of the novel coronavirus, has likely shifted and increased the informational needs of businesses in connection with providing their products and services. For instance, in December 2019, few would have considered restaurants collecting

---

[21] Bernard Marr, "Why Data Minimization is an Important concept in the Age of big Data", *Forbes* (16 March 2016), online: <https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/>.

[22] *PIPEDA*, *supra* note 5 at Schedule 1, s 4.4.

[23] Office of the Privacy Commissioner of Canada, "Ten tips for avoiding complaints to the OPC", (Ottawa: OPC, April 2013), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/02_05_d_55_tips/>.

the names and phone numbers of their guests to be necessary pursuant to the requirements of PIPEDA in carrying out their operations. The onset of COVID-19, however, has shifted how businesses are interpreting and implementing their data collection procedures, and the adequacy and reasonableness of such procedures should be viewed and assessed in light of this new normal.

As part of employing a data minimization strategy, franchise businesses should think critically about the questions below, and how they can amend their data collection policies as a result:

- What information do we reasonably need to collect for the purposes of operating the business?
- How will we ultimately use the data we are collecting? How will we safely and efficiently store the data in the meantime?
- Does the individual providing the information know we're collecting this information, and why we're collecting it?
- What will we do with the data once we have determined we no longer need it? How will we safely delete the data?

Assessing the Adequacy of the Franchisor's Data and Privacy Governance

When granting new franchise agreements, or renewing existing franchise agreements, it is imperative that the franchisor's standard form franchise agreement adequately addresses the question of data and privacy protection and control. Franchise agreements can have terms lasting ten years or more. As a result, many of the legacy franchise agreements do not contemplate the topic of data privacy whatsoever - an issue that should be remedied when franchises come up for renewal. Although each franchise system will have unique needs and specifications that will inform the content of its franchise agreement, franchisors should ensure that their franchise agreements provide an adequate level of clarity and consideration to the issue of data privacy and security, while also providing the franchisor with the ability to enact a sufficient data security regime.

As a starting point, the franchise agreement should specify that the franchisee is responsible for fully complying with the franchisor's privacy policy at all times. The franchisor's franchise agreement and its operations manual should clearly state which parties are responsible for acquiring the customer's consent to collecting, using, and retaining their personal information. It should be specified which party is ultimately responsible for maintaining the safety and integrity of customer data and personal information (bearing in mind that the provisions of the franchise agreement or contents of the manual, alone, will not determinatively answer this question).[24] Moreover, the franchisor's operations manual should clearly specify its requirements for its franchisees with respect to information technology hardware and software standards, including operating hardware specifications and the type and version of anti-virus software that should be used. These requirements should be revisited by the franchisor regularly, to consider whether the requirements remain adequate and current.

[24] David J Allsman et al, "Navigating the Changing Privacy and Data Security Landscape" (Paper delivered at the 52nd Annual Legal Symposium of the International Franchise Association, Washington DC, 5-7 May 2019), online (pdf): <https://www.franchise.org/sites/default/files/2019-05/NavigatingtheChangingPrivacyandDataSecurityLandscape.pdf>.

The manual and the franchisor's initial and ongoing training programs for franchisees should also provide sufficient training, guidance, and operating procedures on data collection, handling, storage, and protection, provide the franchisees with the knowledge and training they need to recognize potential threats and attempts by bad actors to access their systems, and procedures to follow should they be compromised or potentially compromised. This training should provide franchisees with tools to help them recognize "phishing" attempts, which are becoming increasingly sophisticated. Franchisors should ensure that that the franchise agreement and manual specify that the franchisor will be solely responsible for addressing the aftermath of any such compromise, (including preparing and coordinating notifications to the privacy commissioners and affected individuals where this is judged necessary or determined to be required), where it pertains to information controlled by the franchisor and the breach originated with the franchisor or its agents, while the franchisee bears the responsibility in cases where the information affected by the breach is controlled by and the breach originated from the franchisee. In either case, the entity affected by the breach must immediately address its cause, and if the franchisee has strayed from the franchise agreement or manual, the franchisee must immediately return to being in full compliance with the specifications of the franchise agreement and/or manual following such a data breach or other issue. This topic is further explored later in this paper.

Franchisors should also be wary of the high turnover of employees franchisees often face, especially in the context of food and retail businesses. Franchisors should require franchisees to update passwords, logins, and other security measures on an ongoing basis.[25] The actions of even one malicious or disenchanted employee can be enough to compromise thousands of franchised locations.

As a reminder, it is crucial that franchisors do not assume direct and substantial control of, or otherwise be responsible for, the franchisee's employees or operations. If a franchisor exercises a significant degree of control over the franchisee's operations or its employees, it is possible that the franchisor will be deemed to be a joint employer of the franchisee's employee. This can result in increased liability for the franchisor with respect to the franchisee's employee's wages, vacation pay, and other benefits, payroll taxes, and severance pay, among other items. The franchisor should avoid directly controlling, training, or disciplining the franchisee's employees when it comes to data privacy matters, and instead require that franchisees themselves implement data privacy and security training, compliance, and supervision programs for their employees. Franchisors can provide franchisees with best practices and suggested guidelines for implementing such programs, but must not assume direct control of such responsibilities.

Ongoing Review of Franchisee Implementation of POS and Information Technology Systems

While it's one thing to impose requirements on franchisees with respect to data privacy and protection, it's quite another thing to actually ensure that the franchisees are complying with these requirements.

Once the required information technology systems have been specified in the franchise agreement and/or operations manual, or following an update to such requirements, franchisors must ensure that franchisees are actually following through with these requirements. Franchisors should devote

[25] David B Ramsey, "Cyber Center: Cyber-Security Considerations for Franchisors: Protecting the Brand While Avoiding Vicarious Liability", *Business Law Today* (20 July 2016), online, *American Bar Association*: <https://www.americanbar.org/groups/business_law/publications/blt/2016/07/cyber_center/>.

time and energy to ensuring compliance with these requirements; as a best practice, the franchisor should designate a senior individual in its organization as the data privacy and protection officer. This individual should be given a broad mandate to ensure that: the franchisor's operations and processes are up to date and tailored to meet the needs of the system, that the system's franchisees are being provided with technology specifications and best practices to safeguard the interests of their franchised business and the system as a whole, and to ensure that franchisees are complying with the franchisor's requirements on an ongoing basis. While appointing an individual to carry out these functions will come at increased cost to the franchisor, it will help provide the franchisor (and ultimately, its franchisees) protection against liability and reputational damage to its brand, and also align with the legal requirement to appoint a person as responsible for privacy compliance.

As is further explored below, franchisors are an attractive target for hackers and other bad actors as a result of the many different entry points that exist into the system's information technology hardware; the non-compliance of any individual franchisee can prove to be a vulnerability for the franchise system, its franchisor, and all franchisees, as a whole.[26] The sloppiness or non-compliance of even a single franchisee can jeopardize the reputation, brand and profitability of the entire franchise system, including all of its fellow franchisees.

Planning Ahead for Worst Case Scenarios

Franchisors should have an action plan and contingency measures in place to address a potential data breach or malicious parties gaining access to their networks, and to mitigate the damage done by a data breach. This action plan should work in tandem with the requirements of the franchise agreement and the operations manual to ensure that the franchisor and franchisees alike clearly understand their respective roles, correctly evaluate whether they are under a reporting obligation with the privacy laws, and that each party and their employees understand what actions they should, and should not, take following such an incident.

Franchisors would also be well served by investigating other services that can assist them in mitigating the potential damage done by such an attack, or even as a result of a non-malicious system failure. Cyber security insurance policies are designed to help organizations mitigate risk exposure by offsetting costs that occur after a cyber-related security event. Cyber security insurance typically covers expenses incurred from the cyberattack and third party liability to protect costs associated with the impacts on other business. Policies can cover costs and losses associated with business interruption, privacy liability, costs of notifying customers, legal expenses, recovering compromised information and repairing damaged computer systems. [27] However, such policies may have requirements for how the organization responds to a security breach. In the aftermath of a breach, it is important to consult the policy to ensure any requirements it specifies are met, or coverage may be jeopardized. While insurance may help in defraying costs associated with a cyberattack, no insurance can cover reputational damage to the franchisor's reputation and brand following an incident. Appropriate security is not only legally required, but an important preventative measure.

---

[26] Ramsey, *supra* note 25, online: <https://www.americanbar.org/groups/business_law/publications/blt/2016/07/cyber_center/>.

[27] Alicja Grzadkowska, "What is Cyber Insurance?", *Insurance Business Canada:* <https://www.insurancebusinessmag.com/ca/news/breaking-news/what-is-cyber-insurance-115359.aspx>

Another tool available to businesses to mitigate damages caused by a cyberattack or system failure are data back-up systems and services, which allow franchisors to retain collected data in the event that primary servers fail or are not accessible. Back-up servers can be hosted onsite or offsite, depending on the business' preference. Such systems can allow the business to keep operating, even in the event that an increasingly common "ransomware" attack disables all or part of the business' systems, or a systems failure otherwise prevents users from accessing the data in question.

3. Dealing with Third Party Vendors

Private sector privacy laws provide that organizations remain responsible for personal information in their control, including in contexts where it is transferred to a third party for processing. Where an organization engages a service provider to process personal information for it, the organization must use contractual means to ensure that the information remains adequately protected in the hands of the service provider. In essence, the organization transferring the information is obligated to use an appropriate form of data protection agreement in respect of it, or adequate data protection provisions will need to be included as part of the broader services agreement.

The requirements for such an agreement will vary depending on the nature of the information processed, and on its sensitivity. The organization disclosing the data must ensure that it continues to receive adequate protection in the hands of the processor. The privacy laws require that the degree of security be "appropriate" considering the sensitivity of the information.[28] More sensitive information, for example, financial information, will require a greater degree of protection then less sensitive information, such as an email list in a non-sensitive commercial context. For credit card information in particular, the agreement must specify that the processor will comply with the current Payment Card Industry Data Security Standard, and for sensitive information more broadly, appropriate security measures including encryption should be specified. Overall, the contractual arrangements must provide assurance that the service provider has policies and processes in place to adequately provide for the protection of the information being processed.

Security aside, an arrangement with a service provider processing personal information for either a franchisor or a franchisee must place appropriate limitations on the use of the information by the service provider, and must ensure that the franchisor or franchisee retains adequate tools to control the use of the information by the service provider. In practice, these will include limiting any processing of personal information to the purposes set out in the agreement, prohibiting the disclosure of the information without permission, and requiring the service provider to return, or if requested securely destroy, the information on request, or on termination of the agreement. In the event of a security breach, the service provider must be required to promptly report the incident to the franchisor or a franchisee, together with sufficient information on the incident to allow the franchisor or franchisee to assess their own reporting obligations (for example, to any affected individuals and the privacy commissioners). The franchisor or franchisee should seek the contractual right to audit the service provider's compliance with the agreement, and should exercise this right in practice.

[28] *PIPEDA*, *supra* note 5 at Schedule 1, Principle 4.7.

The agreement should either prohibit the service provider from using subcontractors to process the personal information, or must ensure that all of the obligations of the service provider, including audit rights, flow through to any permitted subcontractors.

4. Moving forward: Hot Issues and Practical Advice

Cyber Attacks and Data Breaches: Why Franchisors and Franchisees Alike are Priority Targets for Hackers

Across all industries, cyber attacks are becoming increasingly common. Franchise systems are particularly vulnerable to these attacks as they are, by their very nature, decentralized. In addition to the franchisor's own systems and networks, there is the potential that due to their interconnected nature, each individual franchisee's systems may provide malicious actors with the ability to access the systems of every other franchisee and even the franchisor. In systems that have hundreds or thousands of units, the potential for malicious or unauthorized access increases exponentially, and franchisors should consider how to prevent such access by establishing an appropriate security program.

Furthermore, franchisors and their franchisees are attractive targets as a result of the vast amount of consumer data available to hackers across large swaths of individual businesses employing the same, or similar, systems. This allows hackers to deploy the same tricks of the trade across a wide range of unconnected businesses, resulting in a lower chance of detection. One needs to look no further than at the substantial damage caused by cyber attacks at Sonic Drive-In or Pizza Hut to understand the substantial consequences, be they monetary, legal, or reputational, that these attacks can have on franchise brands. [29]

In a report released by the OPC in October 2019, data breach reports at organizations throughout the country are said to have increased six times since those reported in 2018, and the number of Canadians affected by a data breach is well over 28 million. More than one in five of the data breaches reported involved accidental disclosure, including situations where documents containing personal information are provided to the wrong individual, for example, because an incorrect email was used, or an email was sent without blind copying recipients.[30]

Managing the Aftermath: Brand and Reputational Damage, Civil Liability, and Regulatory Investigations

In the aftermath of a successful cyber-attack on a franchise system, the resulting damage can have serious effects on a franchise system's brand and goodwill. In order to succeed in franchising, a brand must be able to deliver a consistently high level of service and quality across all of its franchised locations. As is eloquently described on the Canadian Franchise Association's website, "with consistent levels of service, the franchise is able to build confidence in the mind of the

[29] Ezra D Church and Hilary L Lewis, "Another Restaurant Franchise Serves Up a Settlement After Data Breach" (22 October 2018), *Well Done* (blog), online, *Lexology*: <https://www.lexology.com/library/detail.aspx?g=49dcbeea-a361-4d89-92c2-c4eeb6e1357e>.

[30] Office of the Privacy Commissioner of Canada, "A full year of mandatory data breach reporting: What we've learned and what businesses need to know", (Ottawa: OPC, 31 October 2019), online: <https://www.priv.gc.ca/en/blog/20191031/>.

customer and this drives people to the brand. Customers gravitate to what they know, what is familiar and what they trust."[31]

By the same token, however, franchise systems which receive substantial negative press due to a data breach resulting from the actions of one lone franchisee, or one lone unsecured network, can instantaneously incur serious harm to the franchise system as a whole. Many current and potential customers will be unable, or unwilling, to differentiate an issue suffered by one franchisee from the entire franchise system. This can have a negative impact on sales, and, consequently, the financial viability of each individual franchisee, which can also affect a franchisor's ability to grow and attract new franchisees. Lastly, if a franchise system stores information such as recipes, proprietary methods or business plans online, this information and can be made available to the public and to competitors through a breach, causing further financial damage.

On top of the damage caused by a successful cyber attack, organizations can also be found liable for insufficient or ineffective cybersecurity practices. For example, a failure to provide adequate security as required by the privacy laws can result in complaints filed by groups or individuals, as well as audits or investigations initiated by the relevant privacy commissioner or other regulatory body.[32] In the aftermath of a security breach, an allegation that the organization provided inadequate security often follow, both where the breach occurred due to inadequate security, and where the matter may be one of "hindsight is 20/20".

Regulatory Investigations

Under PIPEDA, the OPC may conduct an investigation of an organization's privacy practices, either following a complaint by an individual, or on the initiative of the Commissioner if they believe there are reasonable grounds to investigate.[33] The Commissioner may choose to investigate in a case where an organization experiences a high profile privacy-related incident, for example, in the aftermath of a large-scale security breach.

If a franchise system becomes the target of an investigation related to a data breach, the Commissioner can choose to publicly disclose the identity of the organization, which can result in further harm to the organization's reputation, as well as the reputation of its franchisees. Furthermore, if the OPC issues a report setting out a finding that an organization has breached PIPEDA, a complainant (or the Commissioner) can apply to the Federal Court of Canada for an order against the organization mandating compliance with PIPEDA, and awarding damages as a result of the organization's breach of PIPEDA.[34] This can include damages for 'humiliation'. Further, security breaches often lead to a class action against the organization.

---

[31] "What is a Franchise?" *Canadian Franchise Association*, online: <https://www.cfa.ca/lookforafranchise/franchise-tutorial-1-what-is-a-franchise/>.

[32] Lyndsay Wasser, Frank Palmay & Mitch Koczerginski, "Cybersecurity – The Legal Landscape in Canada" (October 2017), *McMillan Cybersecurity Article Series*, online (pdf): <https://mcmillan.ca/Files/203115_Cybersecurity_The_Legal_Landscape_in_Canada_October.pdf>.

[33] *PIPEDA*, *supra* note 5 at s 12.

[34] Office of the Privacy Commissioner of Canada, "What you need to know about mandatory reporting of breaches of security safeguards", (Ottawa: OPC, 29 October 2018), online: <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/> [OPC, "Mandatory Reporting"].

Directors and officers of Canadian organizations can be found guilty of an offence and fined up to $100,000 if they knowingly fail to report data breaches to the OPC. They can also face significant monetary penalties if they authorize, acquiesce in or engage in a violation of CASL, which is described further below.[35]

Civil Liability

Class actions related to information security breaches are becoming increasingly common in Canada.[36] Civil disputes stemming from cyber attacks can lead to lengthy and expensive litigation, large damage awards or settlements costs, and significant reputational harm that typically results from a public lawsuit. Vicarious liability for cyber and privacy related claims is also of concern to employers. Recent case law suggests that vicarious liability may apply not only where an employee has negligently carried out his or her duties, but also where a rogue employee intentionally commits a privacy breach. In other words, the fact that an employee's actions were unauthorized does not necessarily free the employer from vicarious liability.[37] This can be of particular concern to franchisees, given the high rate of turnover for employees, and the fact that new people are accessing electronic systems on a regular basis.

Reporting Obligations

PIPEDA imposes certain reporting obligations regarding security breaches involving personal information. Specifically, PIPEDA requires all businesses to:

1. Report any breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals to the Privacy Commissioner of Canada,
2. Notify those individuals affected by the breaches,
3. Notify any other organizations that may assist in reducing the risk of harm; and
4. Keep records of all breache, even if they determine there is no significant risk of harm.

A business is only required to report a breach if it is reasonable to believe that the breach creates a risk of significant harm to an individual. What is considered "significant harm" covers a wide range of things, from bodily harm to negatively affecting someone's credit record. In practice, the "significant harm" threshold tends to be viewed as a relatively low bar.

Who has the obligation to report?

The obligation to report the breach is that of the organization in control of the personal information. What is considered "control" is not defined in PIPEDA, however, the OPC notes that PIPEDA's

---

[35] Tamara Hunter, Rebecca von Rüti & Tania Da Silva, "What directors and officers of Canadian organizations need to know about potential individual liability for cyber-claims" (16 April 2019), *DLA Piper* (blog), online: <https://www.dlapiper.com/en/canada/insights/publications/2019/04/potential-individual-liability-for-cyber-claims/>.

[36] *Ibid.*; Sarah Dever Letson, "Vicarious Liability for Cyber and Privacy-Related Claims: Is Your Organization Protected Against Internal Threats?" (29 November 2019), *Mondaq* (blog), online:https://www.dlapiper.com/en/canada/insights/publications/2019/04/potential-individual-liability-for-cyber-claims/ <https://www.mondaq.com/canada/Privacy/869358/Vicarious-Liability-For-Cyber-And-Privacy-Related-Claims-Is-Your-Organization-Protected-Against-Internal-Threats>.

[37] Letson, *supra* note 36, online: <https://www.mondaq.com/canada/Privacy/869358/Vicarious-Liability-For-Cyber-And-Privacy-Related-Claims-Is-Your-Organization-Protected-Against-Internal-Threats>.

accountability principal provides than an organization remains responsible for any personal information that it has transferred to a third party for processing. Therefore, even if a breach happens when the information is in the hands of a third party, the principal organization will still be responsible for reporting it. [38] This is especially relevant for both franchisees and franchisors. If data is collected by the franchisor and distributed to the individual franchisees, and the franchisee is victim to a data breach, the franchisor also has reporting obligations.

Record-Keeping Obligations

PIPEDA also requires businesses to maintain a record of every breach of security safeguards involving personal information, whether or not it is required to be reported. These records must include:

- The date (or estimated date) of the breach
- A general description of the breach
- The nature of the information involved in the breach
- Whether or not the breach was reported. [39]

Notifying Individuals Affected by the Breach

Along with submitting a breach report to the OPC, organizations are also responsible for notifying any individual to whom the security breach poses a real risk of significant harm. This notification must be made as soon as possible, and must clearly explain the significance of the breach and provide enough information for the individual to be able to take steps to mitigate the possible harm. Furthermore, the organization must also notify any government institutions or other organizations that it believes could reduce the risk of harm resulting from the breach. This obligation is context specific, for example, organizations should notify law enforcement if they believe bad actors have accessed their customers' information.[40]

Lastly, organizations should develop a framework for assessing the real risk of significant harm. The OPC suggests a two-pronged assessment that considers (1) the sensitivity of the information involved in the breach, and (2) the probability that the information has been or will be misused.[41]

Response Plans

In light of the potential consequence of a cyber attack, it may be very tempting for a franchisor to step in and try to manage all of the risk by itself. However, the franchisor-franchisee relationship prevents franchisors from stepping in to directly manage its franchisee's businesses. Franchisors therefore need to make sure they operate within the context of the franchisor-franchisee relationship to equip the franchisees with the right advice, resources, and assistance to mitigate

[38] OPC, "Mandatory Reporting", *supra* note 34, online: <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/>.
[39] OPC, "Mandatory Reporting", *supra* note 34, online: <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/>.
[40] Anna Thompson-Amadei, "What you need to know about mandatory reporting of breaches of security safeguards" (2 November 2018), *Sotos* (blog), online: <https://sotosllp.com/what-you-need-to-know-about-mandatory-reporting-of-breaches-of-security-safeguards/>.
[41] OPC, "Mandatory Reporting", *supra* note 9.

cyber threats and deal with them if they happen.[42] Franchise agreements and manuals should address how data breaches involving franchisees must be managed, as well as stipulate that franchisees are required to cooperate with the franchisor.

Pre-Attack

Franchisors should review their franchise disclosure documents, franchise agreements and manuals and update them to ensure that they properly address cyber risks. Its possible, and even likely, that older franchise agreements do not expressly deal with cyber risk issues. However, certain provisions may already be in place that are broad enough to address the new risks posed by technology. For example, a provision requiring a franchisee to maintain appropriate insurance may be broad enough to include cyber insurance coverage, or a provision requiring the franchisee to obtain ongoing training may be broad enough to include cyber security training. Franchisors may also want to consider any contracts that are entered into with suppliers, and whether these include provisions that shift the risk of cyber-attacks to the appropriate party.[43]

Having sufficient cyber-attack insurance is one way to help ensure sufficient resources are available to handle the post-attack crisis in a way that minimizes brand damage. For example, cyber attack insurance can cover legal services needed following an attack, as well as the cost of public relations professionals to help the franchise system post attack and forensics (to determine how the attack occurred, and how to repair computer systems).[44]

Post-Attack

Even with every precaution, it is possible to fall victim to a cyber attack. It is important to have a well thought out crisis plan that identifies the most likely risks in the system and contains specific action plans in response to each risk. Major data breaches that involve franchisees will almost always require the involvement of the franchisor to some degree, and any data breach that happens to a franchisor will have an impact on franchisees.

It is important that crisis plans clearly identify which individuals are responsible for managing the different responses. Key responsibilities should be assigned to the person who is in the best position to respond to the risk. A clear and well thought out response plan also demonstrates that an organization has done its due diligence. Pre-drafting communications and other public statements in anticipation of likely attacks, and other table-top exercises to review breach preparedness is a good way to ensure that your organization is ready to handle a cyber attack. Customers affected by the attack will expect to hear an update immediately from the organization, especially during a crisis.[45]

Marketing and Anti-spam Compliance

CASL requires express or implied consent to send commercial electronic messages ("CEM"), including email and text messages. CASL is very prescriptive, requiring specific disclosure to obtain valid express consent, limiting 'implied' consent to certain specifically defined

[42] Adrienne Boudreau, "Cyber Risk" (15 November 2019), *Sotos* (blog), online: <https://sotosllp.com/cyber-risk/>.
[43] Boudreau, *supra* note 42 , online: <https://sotosllp.com/cyber-risk/>.
[44] *Ibid.*
[45] *Ibid.*https://sotosllp.com/cyber-risk/

relationships, and requiring commercial electronic messages to include specific disclosure and an unsubscribe mechanism. These requirements are not intuitive, and can pose additional challenges in the franchise context. Unfortunately, CASL is also extremely punitive, and includes an administrative monetary penalty of up to $10,000,000, which can be imposed following an investigation by the regulator, the Canadian Radio-television and Telecommunications Commission ("CRTC"). As a result, the law warrants special attention by franchisors and franchisees, as it can create potential pitfalls for common business practices.

CASL also casts a very broad net, prohibiting entities from sending, causing, or permitting to be sent CEMs without valid consent or without the content required by CASL. Further, CASL prohibits aiding, inducing, or procuring any act contrary to it. In enforcing this prohibition, the CRTC has indicated that it will consider the level of control that an organization has over the activity that violated CASL, the degree of connection between the actions that could be deemed to "aid" the violation of CASL and those actions that actually violated it, and whether the organization had taken reasonable steps to prevent a violation.[46]

The broad drafting of CASL and the guidance of the CRTC creates potential liability for both franchisees and franchisors who exchange email addresses and send CEMs. For example, regardless of whether the email addresses are initially collected by the franchisee or by the franchisor, if one of those parties provides email addresses to the other, who then uses the addresses in violation of CASL, the entity that provided the email addresses could be targeted for "permitting" or "aiding" a violation of CASL. Conversely, if the party that had initially collected the email addresses had not secured adequate consent, (which as discussed in the following section poses challenges in a franchise context), either that party, or the party using the addresses could be found offside CASL.

As a result, in any scenario where members of a franchise organization exchange email addresses for marketing purposes, responsibility would lie on both parties to ensure that the other is obtaining, and using, those email addresses in a manner compliant with CASL. Failure to do so could result in liability falling on either or both of the franchisor and franchisee, although CASL includes a due diligence defence for organizations that establish they "exercised due diligence to prevent the commission of the offence".[47]

The CRTC has published guidance on what it considers appropriate elements of a corporate due-diligence program that should be considered by franchisors and franchisees sharing email addresses, or by either franchisors or a franchisee seeking to set up their own complainant email marketing program.[48] Corporate compliance programs should include support from senior management, with a clear designation of an individual as responsible for the organization's compliance. The program should establish clear and actionable procedures for CASL compliance, including who within the organization is authorised to send commercial messages, procedures for obtaining and recording consent, processes to implement opt-out requests, employee training, and

[46] Canadian Radio-television and Telecommunications Commission, "Guidelines on the Commission's approach to section 9 of Canada's anti-spam legislation (CASL)", Compliance and Enforcement Information Bulletin CRTC 2018-415 (Ottawa: CRTC, 5 November 2018).
[47] CASL, *supra* note 7 at s 46(2).
[48] Canadian Radio-television and Telecommunications Commission, "Guidelines to help businesses develop corporate compliance programs", Compliance and Enforcement Information Bulletin, CRTC 2014-326 (Ottawa: CRTC, 19 June 2014).

record keeping, monitoring and auditing processes to ensure that the policy is implemented in practice, and that if investigated, the organization can prove it is sending commercial electronic messages in compliance with CASL.

Lastly, any organization's compliance program must be reviewed and updated as the organization, or its practices, change. Simply setting up a paper policy that neither reflects the organization or its practices and that is neither implemented or updated is not much better than not having a compliance policy in the first place.

Consent

CASL requires the consent of the individual before they are sent any CEM. Unlike the private sector privacy laws, which as discussed above, are principles based and require informed consent that will depend on the context such that it is reasonable to think the individual understands what they are agreeing to, CASL is very prescriptive with respect to what must be stated when seeking express consent, and what kinds of interaction give rise to implied consent.

For a request for express consent, CASL requires an express opt-in that states:

1. The purpose of the consent (e.g. sending commercial electronic messages),
2. The name of the entity asking for consent,
3. If applicable, the name of any entity on whose behalf consent is sought, and an indication which entity is asking or the other,
4. The mailing address of one of those entities,
5. Either a telephone number, email address, or web address for one of those entities, and
6. A statement consent can be withdrawn.

Requirements 2 and 3 can pose a particular challenge in the franchise context. If a franchisor were to seek consent for its franchisees to independently send commercial electronic messages in their own right, the franchisees would need to be named in the request for consent. For large franchise operations this would be extremely burdensome. There are separate provisions that allow consent to be obtained for entities whose identity is not known and therefore not stated in the consent language. However, one can query whether the identity of the franchisees is "not known" to the franchisor. Further, these provisions have onerous implementation requirements, including identifying the person who obtained consent in any CEMs sent, and using a form of unsubscribe mechanism that allows the CEM recipient to withdraw consent from the person who sent the message, the person who obtained consent, and any other person whom they authorized to use the consent.

However, there are several approaches that franchisors may consider. First, if it is only the franchisor would be sending the messages, with the franchisees lacking material control over the message content or destination, then only the franchisor would need to be named in the request for consent. This would be true even if the message included information regarding the franchisees, or a particular franchisee, such as a franchisor-controlled 'locator' tool that allows consumers to find nearby franchisee locations.

Secondly, it would be possible to ask consumers to specify their preferred location in the email consent flow, for example, by asking the consumer to select from a list of locations, or provide the first three characters of their postal code. Following that, the consent language could dynamically

display the name and contact information for the nearest franchisee. Likewise, there would be the possibility to use franchisee specific consent language that also sought consent for the franchisor at a franchisee point of sale (for example, by way of tablet).

CASL also recognizes implied consent arising from certain defined "existing business relationships". These include:

1. Where the message recipient has purchased or leased goods or services from the message sender in the two years prior to the message;
2. Where the message recipient has accepted a business opportunity from the message sender in the two years prior to the message;
3. Where the message recipient has an existing written contract with the message sender, or such a contract expired in the two years prior to the message, or
4. Where the message recipient has made an inquiry or application to the message sender regarding a purchase or lease of goods or services or a business opportunity in the prior six months.

For each of the forms of "existing business relationship" that give rise to implied consent under CASL, we note that they exist for the organization that holds the relationship with the message recipient. For example, in a scenario where sales were always made by the franchisees, the franchisor could not typically rely on a purchase from a franchisee to constitute implied consent for the franchisor.

The preceding considerations may push franchisors who do not make sales directly toward express consent to send CEMs. Where they hold the relationship with the consumer directly, the franchisee may have greater flexibility to seek express consent, or rely on implied consent.

Conclusion

The Canadian privacy landscape has evolved substantially in recent years, and potentially more coming in the not-too-distant future, with an increased focus on subjects such as meaningful consent, accountability, and breach reporting. Moreover, the stakes and potential risks have never been higher, with privacy related incidents regularly making the headlines, and with the introduction or proposal of higher penalties, including for common business activities such as sending promotional email.

In this paper, we have highlighted several key considerations for the franchisor/franchisee relationship, which we hope the reader finds of use in entering or updating their franchise agreements or the franchisor's operations manuals, policies and practices.