Anonymous video analytics' future uncertain after Canadian privacy regulators' investigation

November 04, 2020

On Oct. 28, 2020, the federal privacy commissioner and its provincial counterparts in Alberta and British Columbia issued joint findings with respect to the information-handling practices of a property management company using anonymous video analytics (AVA) in order to generate demographic information about consumers in its shopping centres, in a purportedly anonymized and aggregated format.

In this case, sensors were placed in digital mall directories at various shopping centres across Canada. The sensors used facial characterization technology – another name for anonymous video analytics – to extract an estimate of the age and gender of consumers within the sensor's range. Although the company argued that its use of AVA was not subject to Canadian privacy laws in that the technology did not collect personal information within the meaning of those laws, the commissioners disagreed and made a number of important findings with respect to AVA.

In light of the nature of information being collected via AVA in this instance, the commissioners concluded that express opt-in consent would be required, as they determined that some of the information involved was sensitive and its surreptitious collection in this context would be outside the reasonable expectations of consumers.

The company was advised to limit its retention of such information and to update its policies and procedures with respect to obtaining meaningful consent. Although the decision also explored the company's use of mobile device geolocation technologies, the present review focuses on the privacy commissioners' findings with respect to AVA.

Background

In a recent Report of Findings, the Office of the Privacy Commissioner of Canada, in collaboration with its counterparts from Alberta[1] and British Columbia[2] (collectively, Commissioners), issued a confounding decision regarding the legality of anonymous video analytics (AVA) under the federal *Personal Information Protection and Electronic Documents Act* and substantially similar private sector privacy laws in Alberta and British Columbia (collectively, Canadian privacy laws). This decision potentially upends the use of a relatively novel technology that many considered privacy-preserving.[3]

The Commissioners launched a joint investigation into the property management company's information-handling practices, following a number of media reports of consumers' personal information being collected without their knowledge or consent at malls across Canada via sensor-equipped wayfinding directories, *i.e.*, interactive digital maps.

The investigation revealed that the sensors had collected and used images of faces (images), which had been converted into unique numerical representations of those faces (numerical representations of facial features) in order to generate information about the approximate age and gender of consumers (demographic data).

However, the company argued that the AVA technology used – which was installed and managed by a service provider – did not result in any collection, use or disclosure of "personal information" within the meaning of Canadian privacy laws. Rather, the company said, the information collected from the sensor was anonymized, meaning it could not be used, alone or in combination with other information, to identify an individual. As it was not collecting any personal information via AVA, the company argued that it was not required to comply with notice and consent requirements.

What are anonymous video analytics, or AVA?

AVA is a type of technology that aims to generate valuable insights about on-site consumers – such as an approximation of their age, gender and even emotional state relative to a particular digital display – in an anonymized and aggregated format using face pattern detection algorithms to scan real-time video feeds.[4]

Unlike facial recognition, which creates a template of an individual's physical or behavioural characteristics for authentication or identification purposes, AVA is not meant to identify or authenticate individuals, meaning that images collected via AVA are generally processed locally and retained for a very short period (if at all). In theory, no unique, persistent template of an individual's facial features is created or preserved.[5] Given these notable distinctions, AVA is referred to as "facial detection" or "facial characterization." It is often mistaken as a form of surveillance or biometric system, though, as it relies on biometric characteristics and uses similar hardware.[6]

While its use extends beyond the confines of the retail industry, AVA is increasingly associated with the traditional brick-and-mortar store, especially as it seeks to reinvent itself in an effort to compete with e-commerce, a sector that has seen tremendous growth at the expense of traditional retailers.

The unabated rise of e-commerce may be attributed, at least in part, to the online industry's ability to leverage various information-gathering and tracking tools in order to target advertisements to their audience and tailor the shopping experience of consumers, generating valuable metrics along the way. AVA emerged as the "offline" retail industry's response to an increasingly lopsided affair, promising to correct the informational imbalance between brick-and-mortar and online stores. More specifically, AVA is used to produce various consumer metrics in real time, which can be leveraged to create a more frictionless shopping experience, improve product management and business decisions, and measure engagement with visual communications and displays, all while promising to better preserve the privacy of consumers through a "privacy by design" approach.[7]

Decision

The Commissioners' decision relied on a number of key findings with respect to the particular features of the AVA technology used in this instance, the type of information collected and the duration of retention of such information by the service provider. Although the decision also considered these questions with respect to information collected during the pilot phase of the AVA initiative, the present analysis focuses on the company's subsequent rollout of AVA at its malls.

At the outset of their decision, the Commissioners noted that the AVA technology used in this case did not work "entirely in real time" and required images to be collected and stored in memory, albeit for "a very short period of time."[8] Without much debate, this was held to be sufficient to constitute a "collection of personal information" within the meaning of Canadian privacy laws, notwithstanding the fact that images were held in memory for a period that the company described as mere "milliseconds."

Perhaps anticipating that future technologies may render such ephemeral storage of images all the more imperceptible, the Commissioners also noted that information does not necessarily need to be recorded in order to be considered a collection of personal information under Canadian privacy laws. In practice, this will likely cause most types of AVA technologies to be subject to Canadian privacy laws, as AVA necessarily requires and relies on visual sensors.

Turning to the particularities of the AVA technology involved in this case, the Commissioners also found that images were used to generate unique "numerical representations of facial features" (described below) and demographic data, in effect constituting a separate collection and use of personal information. Through an embedding process, images were converted into a unique numerical representation of a particular face, which the Commissioners qualified as "biometric information," an important qualification given the relative sensitivity attributed to such information. Indeed, these numerical representations of facial features were held to be "biometric" in that they were derived from measurements of facial features and could be used for identification or authentication purposes – for facial recognition.

That being said, the Commissioners acknowledged that neither the company nor its service provider had used this information to identify or authenticate an individual. It is relevant to note that AVA technologies are not normally meant to generate these types of unique, persistent "templates" of individuals' facial characteristics, as they are not designed to conduct facial recognition.[9] However, in this case, the Commissioners found that the AVA technology relied on software that could be used for facial recognition, although this particular feature was turned off.

Although the Commissioners agreed that demographic data (*i.e.*, age and gender) could not, by itself, qualify as "personal information" within the meaning of Canadian privacy laws, they took the view that it became "personal information" in the present circumstances, as it was stored with other information that could have been used to identify an individual. More specifically, and unbeknownst to the company, the service provider had stored the demographic data with numerical representations of facial features and circumstantial information – namely the time and location where the picture was originally taken – on a database, without any justification for doing so.

As such, the Commissioners not only took the view that this information qualified as personal information, they also concluded that the company had breached data retention requirements by retaining personal information (*i.e.*, numerical representations of facial features) beyond the period necessary to achieve the purpose for which information was collected, which, in this case, was to generate demographic data, not to track or otherwise identify individuals.

Given the Commissioners' findings that the property management company had collected personal information, the company had to obtain meaningful consent before collecting and using consumers' personal information via AVA. However, in the present circumstances, the company was required to obtain consumers' express opt-in consent, as the collection and use of biometric information was considered sensitive and outside the reasonable expectations of consumers, who would have little reason to suspect their images were being captured and used for such purposes when interacting with a mall directory.

The company was also advised to review its privacy policy and signage, as they provided insufficient detail about the purposes being pursued, the type of information being collected, and how it would be used. Given that the practice was outside consumers' reasonable expectations, it was incumbent upon the company to bring information about its privacy management practices to the attention of consumers in a manner that was both explicit and readily accessible at the time consumers were interacting with wayfinding directories (*i.e.*, at the time of collection). For these reasons, the Commissioners concluded that the company had also violated its obligation to obtain meaningful and informed consent.

Business takeaways

The Commissioners' findings with respect to the company's use of AVA give rise to four important takeaways for businesses relying on similar technologies:

- **Canadian privacy laws apply to AVA technologies.** The decision represents a clear, affirmative statement by privacy regulators that AVA will generally be subject to Canadian privacy laws, as it can be surmised that most AVA technologies are likely to temporarily capture an image of an individual's face before extracting anonymized and aggregated data. The Commissioners were careful in stating that Canadian privacy laws do not require information to be "recorded" in order to qualify as personal information and, in any event, that an image captured in memory even for a split second qualifies as a collection of personal information.
- **Periodically audit and review service providers' information-handling practices.** The decision highlights the importance of periodically auditing and reviewing the information-handling practices of service providers to ensure that they comply with their contractual obligations, including those related to the collection, retention and use of personal information on behalf of an organization. Under Canadian privacy laws, organizations are generally required to enter into a formal written agreement with their service providers – including affiliates acting as such – who handle personal information on their behalf, containing adequate security safeguards that are adapted to the nature, scope and sensitive of the information being processed. In practice, these agreements often contain requirements related to limiting the retention of personal information and grant

the organization a right to audit and review the service provider's activities. Therefore, it is crucial for these rights to be properly enforced in order to reduce risks related to the unauthorized retention and storage of personal information.

- **Evaluate the functions and features of AVA and conduct a privacy impact assessment before implementing.** Organizations using AVA to generate consumer insights should carefully review and evaluate the technology's functions and features to ensure that it does not generate any unique, persistent identifiers that could be used to identify an individual. As previously explained, AVA is not meant to retain images for an extended period of time, nor to generate unique "templates" of individuals' facial characteristics that could be used for facial recognition purposes. Although the Commissioners' findings may have differed had another type of AVA technology been used, it is nonetheless important for organizations to exercise due diligence in evaluating how the technology collects, uses, retains, or discloses information, as this will help reduce privacy-related risks. Incidentally, organizations should consider conducting a privacy impact assessment before implementing these technologies in order to properly identify, evaluate and mitigate those risks.
- **Review existing policies and procedures to ensure transparency and consent.** With respect to notice and consent requirements, the decision is an important indication that organizations will be expected to exercise greater transparency before using AVA, especially as there is currently considerable public distrust and apprehension regarding this technology. This means that organizations should review their existing communication practices to ensure that consumers are adequately informed about the use of AVA at the time of interacting with digital displays equipped with such technologies. In other words, before collecting images of consumers for the purposes of generating insights, consumers should be provided with clear, unambiguous and accessible information regarding the purposes of collection, the type of information collected and how it will be used by the organization. This information may be provided through a variety of communication channels, including physical signage, pamphlets, dedicated pages on the organization's official website, videos, etc. Although the decision recommended relying on opt-in consent, it bears noting that the Commissioners did not necessarily preclude reliance on implied consent with respect to other forms of AVA that do not collect biometric information or other types of sensitive information. As more fully detailed in the section below, the Commissioners' decision was heavily influenced by their determination that the company's collection of numerical representations of facial features qualified as "biometric information," which suggests that AVA technologies that do not collect such information may not require express opt-in consent. That said, as it is crucial to gain the public's trust before implementing this type of initiative, organizations should exercise caution and pay careful attention to how they choose to communicate information about their information-handling practices.

Analysis of outstanding questions

The Commissioners' findings chip away at the viability of AVA in Canada's offline retail sector, as they ostensibly impose on organizations an obligation to obtain consumers' express consent. This requirement is not always realistic nor feasible, especially as doing so may ultimately affect the accuracy and value of the data being generated. Yet, it may be possible to distinguish between the circumstances that led to this decision and other types of AVA technologies, which could be considered less intrusive in their

scope, in order to render reliance on implied consent more reasonable in certain situations. Below, we canvass some of these potential arguments and propose a path forward in implementing these technologies.

Scope of "personal information"

While the Commissioners endorsed a broad interpretation of the meaning of "personal information" and readily concluded that the mere capture of an image, albeit for a millisecond, constitutes collection of personal information, these arguments are likely to be put into question as AVA technologies develop, making retention increasingly imperceptible.

Information will be "about an identifiable individual" where there is a "serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."[10]

The Federal Court recently described this "serious possibility" threshold as, "a possibility that is greater than speculation or a 'mere possibility,' but does not need to reach the level of 'more likely than not' (*i.e.*, need not be 'probable' on a balance of probabilities)."[11] As such, in order to conclude that information gives rise to a serious possibility of identification, a contextual assessment is favoured in which all the facts must be considered and weighed, including "the type of information at issue, the context in which it appears in the records at issue, and the nature of the other information that is available."[12]

In the present circumstances, there may be reason to question whether an image that is retained in a purely transient manner gives rise to a "serious possibility" of identification. There is no realistic possibility of having either the organization or service provider access this information, let alone use it to identify someone before deletion. While this depends on the particular capabilities and security features of the AVA technology involved it is likely to become increasingly difficult to ignore this line of reasoning, as it appears fictitious to state that an image "captured" in this context should be put on equal footing with images captured via surveillance systems. This would not only ignore reality, it would contribute to the false belief that AVA and surveillance are one and the same. In any event, the limited retention of information is a clear risk mitigation strategy that ought to reduce the level of sensitivity of information being collected, and make implied consent more acceptable in the circumstances.

Scope of "biometric information"

Another important aspect of this decision is its interpretation of the meaning "biometric information," as this played a pivotal role in the Commissioners' determination that the company had to obtain consumers' express consent before collecting their personal information. Yet, there are many aspects of the Commissioners' reasoning potentially open to future debate, including the relative sensitivity of biometric information when used for purposes other than authentication or identification.

The Commissioners' finding that numerical representations of facial features qualified as biometric information was based on the fact that this information was uniquely derived from an individual's physical characteristics and could be used to "distinguish between different individuals." This definition, however, does not strictly align with the federal

privacy commissioner's Guidance on biometric information, which consistently refers to such information in the context of systems that enable machines to "recognize individuals, or confirm or authenticate their identities."[13] In other words, it is not clear whether information derived from physical characteristics ought to inevitably be considered "biometric" – and therefore sensitive – in nature if not used in relation to an identification or authentication system.

While the decision confuses these questions – it was revealed that the AVA technology's underlying software could also be used for facial recognition purposes, meaning that the numerical representations of facial features were suitable for identification purposes – it is possible to question whether the outcome would have been the same if the AVA technology did not possess facial recognition capabilities. Indeed, according to the Future of Privacy Forum, AVA does not "routinely create or retain personally identifiable facial templates," suggesting that facial measurements captured by more traditional AVA technologies lack the requisite degree of "uniqueness" and "persistence" to make them suitable for facial recognition.[14]

More broadly, it is also possible to question whether facial measurements are in fact "sensitive" in other circumstances. According to the Commissioners' findings, facial biometric information is considered more sensitive, since "possession of a facial recognition template can allow for identification of an individual through comparison against a vast array of images readily available on the internet or via surreptitious surveillance."[15]

Yet, the federal privacy commissioner stated in its guidance that facial features were in fact less sensitive than other forms of biometric information, such as fingerprints, irises and DNA, because facial features are less distinctive, less stable over time and can be further varied "through cosmetics, disguises or surgery." In addition, the federal privacy commissioner also stated in its Guidance on biometric information that using "templates" or "summaries" of biometric characteristics are more privacy-friendly, as they limit the amount of information retained and may require access to proprietary extraction methods in order to match templates.

While it is true that the "vast array of images readily available online or via surreptitious surveillance" may make individuals more identifiable in relation to their biometric information, this risk should not be overstated or given predominance over countervailing arguments, such as those previously mentioned. In any event, any serious possibility of identification appears particularly limited if facial characteristics are retained only for the purposes of extracting demographic data and immediately purged from the system's memory.

Relying on "implied consent" for anonymous video analytics as a path forward

According to the Commissioners' Guidelines for obtaining meaningful consent, consent may either be express or implied, depending on the circumstances. However, consent must be express where:

- information is sensitive; or

- its collection, use or disclosure is outside the individual's reasonable expectations; or
- it gives rise to a meaningful residual risk of significant harm.

Yet, without much discussion,[16] the Commissioners concluded that express consent was required with respect to AVA, as the technology collected sensitive biometric information in a manner that was outside the reasonable expectations of consumers. It is possible to challenge these findings on at least two fronts, thereby opening the door to "implied consent" in other circumstances. First, these findings may be challenged based on the scope and sensitivity of biometric information in relation to traditional AVA technologies, as discussed above. Second – the focus of this section – they may be challenged based on the "reasonable expectations" of consumers in public places.

While consumers retain a modicum of privacy in public places, this expectation is likely to be quite low, especially in locations where they are already well aware that they are being filmed by surveillance cameras. In decisions regarding the use of surveillance systems, the public nature of the location being filmed is cited as a factor that lowers individuals' expectation of privacy.[17] Thus, the collection and use of images should not, in and of themselves, justify having to rely on express consent, especially if this information is retained for a very short period of time, is not being constantly monitored or otherwise accessed and is not used for facial recognition purposes. In this sense, AVA is generally no more intrusive than relying on surveys conducted onsite. Unlike AVA, these surveys are considerably more expensive and may not be as accurate.

It bears noting that what constitutes a "reasonable expectation" of consumers is an inherently value-laden assessment that is likely to change over time. Take, for instance, the information captured online about users, as they browse the internet. For one, online tracking tools are considerably more invasive and persistent than AVA, as they permit users to be tracked, profiled and targeted. Yet, these technologies are more widely known – and arguably accepted – by the public. In contrast, consumers may not be fully aware of what AVA is or how it may be used, leading to considerable confusion and distrust towards these technologies, which are often seen as synonymous with facial recognition. This distrust provides perhaps a more salient argument for enhancing transparency and providing consumers with better, clearer and more accessible information regarding an organization's use of AVA.

Conclusion

Overall, the circumstances underlying this decision were less than ideal for evaluating the merits of AVA, as the technology involved in this case purportedly shared certain features with more privacy-intrusive technologies such as facial recognition. The legality of AVA under Canadian privacy laws is made somewhat uncertain as a result of the Commissioners' findings, and it is unclear whether the outcome would have been different had another form of AVA been addressed by the Commissioners.

While it may be possible to rely on consumers' implied consent in certain circumstances, this decision highlights the importance of moving away from a consent-centric model of privacy towards one that recognizes multiple legal bases for processing personal information – a solution that the federal privacy commissioner endorsed in its recent appearance during public consultations on Québec's privacy law reform. This approach is neither novel nor radical, as it is precisely the approach taken by the European

Union's *General Data Protection Regulation*, which provides six distinct legal bases on which personal data may be processed, including the legitimate interests of businesses, subject to robust transparency protections and data subject rights.

In the present circumstances, it may simply be unrealistic and unnecessary to obtain consumers' express consent with respect to AVA, especially when used to passively collect information about consumers. For instance, AVA may be used to measure the gaze and facial expression of passersby in order to determine the effectiveness of a digital advertisement – consumers are only passively engaging with the display. In these circumstances, it is considerably more challenging to rely on consent, whether express or implied, without distorting the meaning of this notion.

For the offline retail industry, the present decision may ultimately be seen as a major blow in their efforts to compete meaningfully with e-commerce, as it may unduly constrain their ability to gain valuable insights about consumers and adapt their practices to render the in-store shopping experience more frictionless and convenient. As this digitization of retail is only expected to accelerate, due in part to COVID-19's impact on consumer behaviour, which by some accounts is likely to have some permanence,[18] it is clear that brick-and-mortar stores must be given the proper tools to innovate in order to remain competitive.

While consumer privacy remains critical to the viability of these initiatives, these interests must be realistically evaluated and weighed against the scope, nature and consequences of the information-processing activity.

BLG's Cybersecurity, Privacy & Data Protection lawyers are available to answer any questions you may have about use of anonymous video analytics in Canada. Reach out to your lawyer or any of the key contacts below for assistance.

[1] Office of the Information and Privacy Commissioner of Alberta.

[2] Office of the Information and Privacy Commissioner for British Columbia.

[3] Information and Privacy Commissioner of Ontario, White Paper: Anonymous Video Analytics (AVA) technology and privacy, April 2011.

[4] Information and Privacy Commissioner of Ontario, White Paper: Anonymous Video Analytics (AVA) technology and privacy, April 2011, page 3.

[5] Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications, September 2018, page 1.

[6] Future of Privacy Forum, Understanding Facial Detection, Characterization and Recognition Technologies, March 2018.

[7] Information and Privacy Commissioner of Ontario, White Paper: Anonymous Video Analytics (AVA) technology and privacy, April 2011.

[8] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2020-004, paragraph 62.

[9] Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications, September 2018.

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

[11] *Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness)*, 2019 FC 1279, paragraph 53.

[12] *Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness)*, 2019 FC 1279, paragraph 67.

[13] See also Commission d'accès à l'information, Biométrie : principes à respecter et obligations légales des organisations, July 2020, page iv.

[14] Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications, September 2018.

[15] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2020-004, paragraph 79.

[16] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2020-004, paragraphs 79-81.

[17] *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, paragraph 180.

[18] US e-commerce sales are expected to reach $1 trillion in 2022, roughly two years ahead of earlier estimates, due in part to COVID-19.

By

Andy Nagy

Expertise

Cybersecurity, Privacy & Data Protection, Privacy & Security Breaches, Technology

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749