A Canadian privacy perspective on the commercial use of anonymous video analytics in public settings

June 08, 2021

In October 2020, Canadian privacy regulators issued their findings and recommendations concerning the collection of video images of mall visitors for the use of Anonymous Video Analytics technology (or "AVA" for short) installed in wayfinding directories–a type of digital display used by visitors to navigate malls–by a prominent commercial property management company.[1]

In essence, regulators concluded that this technology generated and retained visitors' demographic data, such as their age and gender, as well as their biometric information, a unique numerical representation of facial characteristics that could theoretically be used for facial recognition, without valid consent. This outcome was preceded by a similar decision issued in May 2020 by the Quebec privacy regulator in which it expressed concern regarding the technology's "low social acceptability". Without concluding whether AVA technology complied with the provincial privacy legislative framework, the Quebec privacy regulator also questioned the overall "proportionality" of the collection and use of video images via AVA technology for marketing purposes.[2]

Following the outcome of these decisions and the ensuing negative media coverage, many organizations in the advertising and retail space feared for the future of AVA technology in Canada. Yet, far from being a foregone conclusion, this bulletin describes a number of practical recommendations that provide a path forward for organizations wishing to use AVA technology in public settings, such as malls, retail outlets, museums and other venues for commercial purposes, including advertising, resource management and statistical purposes. Notwithstanding our belief that a path forward exists for the commercial use of AVA, there are two key challenges from a privacy perspective in the short term:

1. social acceptance concerns arising from the novelty of AVA as deployed in a public setting; and
2. stigma arising from the media and regulators conflating facial *detection* with truly invasive facial *recognition* technologies.

Organizations will have to address these challenges in tandem to mitigate privacy concerns and legal risks related to the use of this technology. To this end, organizations should expect to devote extra time and resources to the following elements:

- Educating the public about AVA, how it operates, what type of data is collected, for what purposes and why this technology is useful. Particularly, paying attention to distinguishing AVA from other more intrusive types of technology, such as facial recognition; and
- Building trust through transparency and creative engagement with stakeholders via a multi-pronged communication and awareness plan, including but not limited to clear, prominent signage in areas equipped with AVA technology.

What is anonymous video analytics?

Anonymous Video Analytics (AVA) describes a type of technology that collects video images using camera sensors (often, but not always embedded in digital displays) to detect the presence of a human face. It then derives limited demographic and behavioural data about viewers (*i.e.* those who come into the field of view of the sensor) using facial pattern comparison algorithms. For instance, this may include data about the number of individual visits in an area over a given period (*i.e.* footfall), the viewer's approximate age and gender, and the amount of time spent looking at the digital display. The technology may even provide a crude estimate of the viewer's mood, but this indicator is more of a "guesstimate" of whether a person looked happy, unhappy or unfazed when viewing the displayed content. Unlike the technology described in PIPEDA Report of Findings #2020-004, this normally occurs without identifying an individual, generating any type of face-based signature, or otherwise generating information that could be associated with an identifiable natural person–hence the term "anonymous". Once the system generates demographic and behavioural data, images are automatically and permanently deleted from its memory. This process typically happens within a fraction of a second. Then, the remaining data is aggregated in predetermined time segments (*e.g.*, 15-minute segments) to gain valuable insights into the audience sample.

Why is anonymous video analytics useful and legitimate?

The data generated with AVA may be used for a variety of purposes. Most often, the technology is used in public settings, such as malls and public transit to:

- Measure viewer engagement and interest to improve digital displays and signage;
- Measure viewer demographics, such as age and gender to justify the ad-space value and manage ad-content scheduling;
- Forecast trends and traffic patterns in commercial public areas, such as malls and public transit, to improve resource allocation and management; and
- Enhance health and safety measures.

These purposes are often justified from a commercial, economic and public health perspective, and Canadian privacy regulators have generally been receptive to these

arguments. For instance, the Quebec privacy regulator commissioner expressly recognized the legitimacy of pursuing marketing objectives and learning more about one's customers.[3] Similarly, the federal privacy commissioner underscored in previous decisions the importance of adapting an organization's commercial practices in order to remain competitive.[4]

In the present context, AVA technology is seen as a valuable and cost-effective tool for brick-and-mortar businesses. It helps them remain competitive, create new revenue opportunities, offer customers an increasingly convenient and personalized shopping experience that better responds to shifts in consumer behaviour and competition from online retailers–developments that the COVID-19 pandemic has undoubtedly accelerated. Unlike online retailers, who use a variety of passive tools to amass large volumes of data about their target demographics, brick-and-mortar stores suffer from a comparative lack of data and experience more friction when gathering data in person. AVA is one type of solution that can help traditional retailers remain competitive without sacrificing individual privacy. It does so by generating anonymous and aggregated data that delivers insights about customers' interests, preferences and behaviour, which are used to inform decision-making, maximize revenue opportunities, and improve the overall shopping experience.

While the identified purposes for brick-and-mortar retailers are legitimate and common in other forms of advertising media, the actual risk to privacy created by AVA is perhaps more apparent than real. Video images are deleted within milliseconds of being collected and are only used to generate aggregated data that cannot reasonably be associated with (or otherwise give rise to a serious possibility of identifying) a particular individual. Moreover, putting aside the technology itself, it is generally accepted that individuals have a reduced expectation of privacy in public settings, which further limits the privacy impact of AVA when used in those settings. Given the discernable benefits of this technology, the comparatively limited risks, and the balance that Canadian privacy law seeks to strike between the right of privacy and the need of organizations to collect, use or disclose personal information, it is reasonable in the circumstances to conclude that the use of AVA technology can be justified, subject to certain conditions discussed below.

Key recommendations for the commercial use of anonymous video analytics

In order to mitigate potential legal risks arising from Canadian privacy legislation, commercial organizations that capture and process video images for the use of AVA technology in public settings should consider implementing the following recommendations:

1. Identify the purpose(s) for which your organization is using AVA technology and conduct a Privacy Impact Assessment early on in the development of such initiative.

An organization should identify the specific purpose(s) for which it collects video images for the use of AVA technology. Once identified, it should be able to demonstrate that this purpose is reasonable in the circumstances. Under PIPEDA and substantially similar

private-sector privacy legislation in Quebec, Alberta and British Columbia, the reasonableness of a purpose is evaluated by looking at a number of contextual factors from the perspective of a reasonable person. Although these factors will vary depending on the applicable legislation, an organization should typically consider the following questions before deciding to use AVA technology:

- Is the collection of video images for the use of AVA technology necessary in order to achieve a substantial, pressing and legitimate purpose?
- Will the use of AVA technology efficiently respond to your organization's needs?
- Is the invasion of privacy proportional to the benefits of such technology?
- Is there a less privacy-intrusive alternative available in the circumstances to achieve the same ends (at a comparable cost)?

Key challenges raised by Canadian privacy regulators concern the overall social acceptability of capturing video images for marketing purposes and the reasonable expectations of customers who may be unfamiliar with this technology. It is important to keep in mind, however, that these challenges are not unique to AVA, as it also applies to other novel technologies that involve processing of personal information, such as AI and algorithmic decision-making. Yet, a fear of novelty should not become an undue barrier for innovation and technological development, as this would be inconsistent with the overarching purpose of Canadian privacy legislation. As previously mentioned, its aim is to strike a balance between the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information.

In these circumstances, an organization should carefully develop and document a robust business case for implementing AVA technology and should be able to demonstrate to customers and regulators that this technology is minimally intrusive and genuinely necessary in order to pursue a legitimate, pressing and substantial objective. To this end, Canadian privacy regulators typically recommend preparing a Privacy Impact Assessment ("PIA" for short), which is a document that records and evaluates a particular data processing initiative's compliance with applicable privacy requirements. In essence, this helps an organization identify and mitigate potential privacy risks early on in the development of an initiative that involves processing of personal information. In turn, it provides an opportunity to carefully consider the nature, scope and purpose(s) of an initiative, evaluate its reasonableness, and test the strength of the business case. If the organization's business case is weak relative to the impact the technology could have on the privacy interests of customers, then the organization must either implement additional measures to reduce the privacy impact to an acceptable level or abandon the AVA initiative altogether. The recommendations below are some examples of measures that an organization should consider implementing in order to reduce the impact of an AVA initiative on individuals' privacy interests.

2. Perform due diligence before choosing a particular AVA technology vendor and monitor the vendor 's compliance with privacy requirements

An organization is responsible for personal information in its possession or custody, including information shared with or collected by a third party vendor. As a result, the organization must ensure (generally through contractual means) that this information will receive a comparable level of protection while the vendor is processing it. More

practically, an organization should consider implementing the following steps when selecting an AVA technology vendor:

- Perform reasonable due diligence when selecting an AVA technology vendor to ensure that the technology chosen does not retain video images longer than necessary (ideally, it should delete images immediately after demographic and behavioural data is generated). Most importantly, it should not generate or otherwise retain any identifiable, sensitive information, such as biometric data (*e.g.*, a unique numerical representation of an individual's facial characteristics);
- Obtain a contractual undertaking (commonly referred to as a "data protection agreement") from the technology vendor to respect certain privacy-related requirements, such as restrictions on the use of personal information, organizational, technical and physical safeguards (*e.g*. encryption of data in transit and at rest), data retention limitations, and security incident notification obligations, among others; and
- Monitor technology vendor's compliance with its contractual and legal obligations through periodic audits, surveys and interviews. The data protection agreement with the vendor should expressly include the organization's auditing and monitoring rights.

3. Notify customers about the use of AVA technology in a manner that is more apparent and detailed than the notification traditionally used for video surveillance and proactively engage with relevant stakeholders

An organization should develop various methods of communication/notification to rely on customers' implied consent for the collection and use of video images via AVA technology. Canadian privacy legislation is based exclusively on a notice and consent model. Valid consent requires an individual to reasonably understand the nature, purpose, and consequences of collecting, using or disclosing their personal information. In addition, according to the federal privacy commissioner's *Guidelines for obtaining meaningful consent*, consent may be either express or implied depending on the sensitivity of the information being processed and the reasonable expectations of an individual. While express consent is not typically required (nor practicable) when engaging in traditional video surveillance, implied consent must be obtained by adequately informing an individual via appropriate signage placed at entrances and near areas under surveillance, as per the federal privacy commissioner's *Guidelines for Overt Video Surveillance in the Private Sector*. However, a key distinction between traditional video surveillance and AVA technology is that an individual is much less likely to be aware of the purposes for which video images are captured and used by AVA-embedded cameras.

Given the public's anxiety towards mass surveillance and facial recognition, and a relatively poor understanding of the role and value of AVA technology, an organization seeking to implement this technology should invest extra time and resources educating the public about this technology to build trust and social acceptance around its purposes and use. This approach involves a greater degree of transparency than that typically involved in video surveillance. It may even require proactive engagement and marketing strategies to interact with customers and other stakeholders. Ultimately, an organization relying on implied consent must be in a position to demonstrate that all individuals would likely have seen, heard and/or read, and understood the notification before or at the time

of collection of their image (i.e., the nature, purpose and consequences of the information processing involved).

4. Provide customers an opportunity to avoid areas equipped with AVA technology without preventing access to related products or services

An organization should consider limiting AVA technology in areas that an individual must traverse to access certain products or services. Although this will vary depending on the location and AVA technology used, this will likely include areas such as entrances, exits and elevators. Similarly, suppose an organization relies on implied consent to use AVA-embedded interactive digital displays designed to provide a particular service, such as wayfinding directories. In that case, they may also have to provide customers with a reasonable alternative to access the specific (or equivalent) service without being subject to AVA technology.

5. Develop a standard operating procedure for the implementation and use of AVA technology and identify the individual(s) accountable for your organization ’s compliance with privacy requirements

An organization should develop a standard operating procedure that governs the implementation and use of AVA technology. At a minimum, this internal document should provide guidance regarding the following aspects:

- The areas in which AVA-embedded displays can or cannot be placed (and related rationale);
- The field of view of cameras;
- Access privileges and the limited circumstances under which such access to video images may be granted to an individual (*e.g.*, troubleshooting, technical support, etc.); and
- The individual(s) accountable for the organization’s compliance with applicable privacy requirements and for handling requests, inquiries and complaints related to the organization’s privacy practices.

An organization should also provide members of its personnel, especially those interacting directly with customers, appropriate training regarding these procedures to ensure that they can answer basic questions about the organization’s information handling practices and, if necessary, escalate privacy-related requests or complaints to the appropriate individual(s).

6. Update your organization ’s privacy policy, using clear and plain language, to include information about the collection of video images for the use of AVA technology and the purposes being pursued

An organization should update its privacy policy to inform customers that video images may be collected at its establishments for the use of AVA technology. Furthermore, it must specify the purposes for which this technology is used; this may require greater transparency concerning the types of demographic and/or behavioural data being generated, how information is used and with whom it is shared. Given the public’s natural lack of awareness of novel technologies, an organization should use clear and

plain language and allow individuals to access and find relevant information easily. For instance, AVA signage could include a QR code to help customers access relevant portions of the organization's privacy policy to learn more about its use of AVA technology. This type of layered approach enables customers to control the amount of detail they wish to receive, as per the federal privacy commissioner's *Guidelines for obtaining meaningful consent*.

7. Conduct ongoing monitoring of the risk of re-identification to ensure that the data generated by AVA technology remains anonymous

Although the demographic and behavioural data generated by AVA technology is typically aggregated in predetermined time segments (*e.g.*, 15-minute segments) in order to reduce the risk of re-identification, an organization should monitor this risk on an ongoing basis to protect the identity of individual customers and maintain the anonymous nature of the information being generated. For instance, an organization should ensure that demographic and behavioural data cannot be combined or otherwise associated with other data sets (*e.g.*, CCTV footage) and should consider limiting the amount (or specificity) of the data being generated. It should also consider combining or increasing time segments used to aggregate this information during periods of low foot traffic.

8. Conduct pilot testing of the AVA technology to ensure that any unanticipated issues are caught early on and properly addressed

Finally, once these measures mentioned above are in place, an organization should also consider conducting a test run of its AVA technology at designated locations to identify unanticipated problems with the technology itself or challenges in how it is implemented. This type of pilot testing may include conducting customer surveys and interviews at fixed intervals to assess the adequacy of the organization's measures. This evaluation may help prevent or mitigate potential issues from arising after officially deploying the AVA technology on a broader scale.

Concluding remarks

The commercial use of AVA technology in Canada remains viable under current federal and provincial privacy regimes. However, in recent decisions, Canadian privacy regulators have effectively put the industry on notice regarding the importance of respecting certain key privacy principles, such as purpose specification, data minimization, use and retention limitations, transparency, accountability and consent. While the present bulletin offers a number of recommendations related to the implementation of these principles, the legitimacy and social acceptability of AVA technology will require a concerted effort to educate and inform the public and build (or perhaps more accurately, rebuild) trust.

[1] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2020-004, October 28, 2020.

[2] Commission d'accès à l'information, Enquête sur l'utilisation de la technologie d'analyse de vidéo anonyme, Dossier 1019951-S, May 15, 2020.

[3] Commission d'accès à l'information, Enquête sur l'utilisation de la technologie d'analyse de vidéo anonyme, Dossier 1019951-S, May 15, 2020, at page 5 : "In this case, the objective is commercial and seeks to develop a technological tool allowing merchants to have an overview of consumers based on attributes such as an estimation of age and gender. These elements allow merchants to better understand their clientele and to adapt their business accordingly. **It is legitimate for a commercial enterprise to have marketing objectives and to want to better know and understand its customers** [our translation]".

[4] See for instance, Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2006-351.

By

Andy Nagy

Expertise

Corporate Commercial, Cybersecurity, Privacy & Data Protection

---