• Age bracket: Young Adult
• Gender: Male
• Distance: 12 ft
• Attentive?: Yes
• Age bracket: Adult
• Gender: Female
• Distance: 8 ft
• Attentive?: Yes
• Age bracket: Adult
• Gender: Male
• Distance: 4 ft
• Attentive?: Yes
Millions of pixels per second are analyzed to detect general traits of viewers anonymously.

White Paper: Anonymous Video Analytics (AVA) technology and privacy

How digital screen network operators are using pattern detection technology
to understand viewing audiences while respecting consumer privacy

April 2011

www.privacybydesign.ca

Information and Privacy Comissioner,
Ontario, Canada

Commissioner's Message:

Tracking individuals online for marketing and other purposes has become a contentious public policy issue for consumers, regulators and advertisers. The stakes are high, and the technologies complex, but by applying Privacy by Design principles early and systematically, privacy, consumer trust, personalization, innovation and economic benefits may all be achieved. This is positive-sum thinking at its best.

Just as ubiquitous and economically dynamic — but far less contentious — is personalized "offline" display advertising to consumers in the "real world." This paper describes innovative digital signage technology, developed in Ontario, that embraces Privacy by Design principles by providing customized content to consumers without identifying them. It is a model approach and solution that offers important illustrative lessons for the online industry.

In the online world, "contextual" advertising is generally understood to be more privacy-respecting than "behavioural" advertising, because it does not identify, track, or profile specific individuals in order to select and display relevant content. The digital signage solutions described in this white paper are the offline equivalent of contextual advertising – there is simply no tracking of individuals across multiple domains, and no identification – ever.

The signage technologies rely upon sensors and software that are able to detect the presence of individuals, and analyze face and body characteristics, to display appropriate informational content in response. Although similar to biometrics technologies which seek to match and identify individuals, these are detection, not identification, sensors. This is analogous to voice recognition versus identification commonly used in interactive telephony systems: common words are understood, but not the identities of the people speaking them.

Here is the privacy bottom line: there is no personal identification, tracking or profiling of individuals by these systems – none. My office supports innovative new privacy-enhancing technologies that offer such positive-sum, "win-win" solutions for all interests and stakeholders, and strongly encourages retailers to follow through on the leadership shown by Intel and others, and to abide by a strict code of privacy standards in their deployment and use. Beneficial innovations in the retail sectors and widespread consumer acceptance depend vitally on ensuring that the virtuous circle of accountability and trust is not broken.

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner of Ontario, Canada

I wish to gratefully acknowledge the assistance and contribution of Intel Corporation in the preparation of this white paper.

Introduction:

Networked digital screens are now prevalent in the retail and public spaces landscape in North America and globally, displaying information and marketing messages to consumers throughout their busy days.

Hundreds of networks, operating hundreds of thousands of Internet-connected screens, have been deployed by everyone from pure startup companies to major media corporations. An entirely new medium has bubbled up and now competes for the advertising budgets of major brands and their media planning agencies. Just a decade old, the Digital Out Of Home (or DOOH) advertising category was estimated by research firm PQ Media to be a $6.5 US billion business in 2010.

Using the same enabling technologies, retailers, packaged goods brands and the operators of facilities such as malls, event centers, airports, colleges and museums are also deploying digital displays to more effectively, and efficiently, communicate with their guests and visitors. Screens intended to influence consumer decisions or simply help people navigate large and busy environments are now commonplace. The digital signage sector, as it is generically known, has developed into a high growth business sector, spawned the development of hundreds of software companies, and drawn in the likes of Intel, Cisco, HP, along with all of the display industry's biggest players.

Whether for advertising, or for other business or communications reasons, these screens are there to engage, inform and entertain viewers. Getting a return on the investment or communications opportunity of these networks is entirely contingent on running content people will see and remember, and on understanding the dynamics and characteristics of the viewing audience.

Measurement of audiences – once little more than estimated percentages of raw foot traffic through venues – has grown to be far more sophisticated in the last five years. One of the most advanced technologies uses sensors integrated with flat panel displays to detect and count the number of faces that look in the direction of the screens. The technology is also increasingly adept at parsing detected faces by gender and age range.

Called Anonymous Video Analytics (or AVA), the technology uses pattern detection algorithms to scan real time video feeds, looking for patterns that match the software's understanding of faces. The data is logged and the video destroyed on the fly – with nothing in the process recognizing the individuals who passed in front of the sensors.

The analytics generated by AVA systems are giving marketers and business communicators valuable new insights into the numbers and characteristics of the audience, including viewing patterns. AVA reports indicate what's actually happening within the proximity of displays, and helps communicators improve on what they're doing.

The presence of sensors and the ability to mine consumer behaviour data has attracted the attention of privacy advocates, who want to understand the technology and its implications. Face pattern detection technology is not designed to recognize (or capable of recognizing) individuals, but it is still gathering data on consumer viewership behavior. It is incorrectly perceived at times to be in the same technology family as surveillance and biometrics that can recognize, log and track individuals. With references to Orwell's Big Brother and Hollywood films such as "Minority Report", AVA has been painted – at times – as the first alarm for a world of signs that are watching people and steadily telling each of them what to buy and do.

In this white paper, the technology and real-world application of AVA pattern detection technology is explored, as well as efforts by technology firms such as Intel to apply Privacy by Design principles to its product development and service delivery. The paper also explores efforts by the technology's user base – ad networks, retailers, brands and complementary vendors – to develop guidelines that responsibly deploy AVA and ensure consumers understand and accept its use.

How AVA works

Sensors located with display panels, or embedded in their fascia, scan the field of vision near screens and send real time video feeds to a computing device. Anonymous video analytics software loaded on that device processes the feed to detect whether arrangements of pixels resemble the general pattern of human faces, using such factors as the pixel density and alignment around eyes.

Those detection algorithms are based on the software having statistically "learned" face patterns, by being trained on an audience database of thousands of face images. The data it compiles includes numbers of faces (also known as "impressions"), timing and the duration that faces look, location in the field of view, size of faces and estimated gender and age bracket.

Each video frame is processed to detect the presence of faces, and is then destroyed in real time. The algorithm does not have the capability to recognize individual faces, and there is no database used to match faces against, as would be the case with facial recognition technology.

The anonymous data aggregated by the software is used to generate malleable reports that provide a clear, accurate understanding of the overall audience. The real time data analysis also opens up the possibility for marketers to do a better job of tuning the messages to viewers. For example, when women are detected to be looking at a screen, mapping AVA data against a real time media player means a hair coloring ad can be dynamically served. When the technology detects a male viewer, the player can be configured to instead serve a shaving product ad.

End-users are applying AVA as a means to make their marketing and communications efforts more effective, by understanding how long their messages should be (based on detected average viewing times), which messages seem to attract and hold people longer, and the characteristics of the audience by time of day and days of the week. Expensive field research to profile audiences at venues might get done once a year, or less, relying on extrapolation and data sampling and therefore providing limited feedback and only a snapshot in time. AVA allows more accurate research to be continuously done, with the results spun back in real time. AVA provides analytics that help media buyers understand how well booked ads perform, all the way through a campaign.

AVA is also giving marketers the ability to assess the cause and effect of marketing messaging, mapping sales or other data against audience data.

AVA in use

The possibilities for applying this technology are vast and steadily evolving, and there are already intriguing, real-world examples of how AVA is being applied.

In Canada, a digital screen network installed in a major grocery chain uses the Intel® Audience Impression Metric Suite (Intel® AIM Suite) technology to optimize the messages for brands sold in the health conscious grocery chain. The sales promotion and information network fine-tunes marketing messages for sponsor brands based on viewer patterns that are tracked using sensors mounted above each screen. The analytics are granular to the level of store zones and messaging, providing data on what messaging works best and where. The network steadily fine-tunes its messages and targeting based on what AVA is telling the operators.

Kraft Foods and Intel have tested and demonstrated in the United States a retail-focused Meal Planning Solution center that allows shoppers in grocery environments to obtain recipes, shopping suggestions, promotional coupons and product samples in a two-way, immersive setting that layers in technologies such as touch screens, 2-D bar code scanners, and mobile. The digital signage screens use AVA to gather retail intelligence on how many shoppers interacted with the self-serve kiosk and for how long, and provides breakdowns on things such as gender, age, and time of day. AVA gives the Planning Solution immediate feedback on ROI and allows content to be adapted in real time and served based on the audience type watching.

At Issue: Consumers being "watched" – Not!

Face pattern detection technology ensures consumer anonymity, but the technology is nonetheless aggregating data on consumer behaviors in the settings where it is deployed.

Though personal privacy is not at risk, market research in the United States has regularly demonstrated most Americans object to marketing tactics that target advertising based on consumer behavior patterns.

Privacy advocates also raise the "slippery slope" argument – that what poses no privacy risk as it now applies could change as technologies evolve. Facial recognition systems and other consumer technologies such as smartphones and RFID embedded smart cards could, in theory, tailor marketing to the purchasing patterns or other characteristics of recognized individuals.

AVA is not designed to do any of that, but there are still suggestions its users need to do more to inform consumers about what's going on.

Getting ahead of the issue

The Digital Out Of Home, digital signage and self-service sectors – all early adopters of AVA – are being actively encouraged by privacy experts to develop and adopt guidelines on its proper use. By getting ahead of the issue – clearly stating and demonstrating how the technology is applied and privacy is protected – vendors and end-users are in the best position to make the most of the capabilities and operate without controversy.

Some technology firms recognized the looming issue early, developing and then publishing their own privacy and consumer protection policies. Intel, for example, clearly states that its AIM Suite system ensures any data detected and aggregated cannot be associated or otherwise linked with any specific individual, and that no personally identifiable information is collected. The company developed its policy using the foundational principles of the *Privacy by Design* guidelines, put together by the Information and Privacy Commissioner of Ontario, Canada.

Because of the increasing complexity and interconnectedness of information technologies, *Privacy by Design* advises privacy be a fundamental part of system design, not something considered later. The seven core principles reinforce the need for both vendor and deploying organizations to operate with transparency and approach privacy as the default setting for a new product or service.

Retaining the public trust

The user base of the industry at large, guided by the U.S.-based Center for Democracy and Technology, has also developed and released its own set of voluntary but strongly recommended guidelines intended to retain the public trust and see best practices recognized and employed.

Building privacy into digital signage business models and data management practices, suggests the non-profit Digital Signage Federation in its privacy guidelines, is the "best way to prevent privacy risks before they arise. This is at the heart of Privacy by Design – avoid the harm. It will be far less expensive for digital signage companies to integrate privacy controls now, while identification technologies are still relatively new to the industry, than it will be to retrofit privacy protections onto future systems."

The DSF's guidelines, released in 2011, broke down the types of information being collected into three categories:

- **aggregate data**, such as the general audience count and profile metrics from AVA systems;
- **pseudonymous data**, such as touch screen logins; and
- **directly identifiable data** such as names and addresses – the sort of information that most concerns privacy experts.

The DSF - which represents a wide range of companies from hardware and software vendors to retailers and fast food restaurant operators - has recommended a set of privacy standards based on the internationally-used Fair Information Practices (or FIPs), which are incorporated in many privacy laws globally.

Those standards recommend:

- **Transparency**: Companies should give consumers "meaningful notice" where the technology is in use;
- **Individual Participation**: Consumers should have the right to opt out (with AVA, notice on site means consumers can choose to avoid the screens and sensors);
- **Purpose Specification**: Published policies should explain how the collected data is used;
- **Data Minimization**: Companies should limit their data collection and retention to only the minimum needed to achieve specified needs;
- **Use Limitation**: Collected data should not be shared or sold for any uses that are incompatible the original purposes specified;
- **Data Quality and Integrity**: If identifiable data is retained, consumers should have the right and mechanism to edit that data for accuracy;
- **Security**: Any data collected should be secured;
- **Accountability**: End-users should establish internal accountability mechanisms.

The guidelines are voluntary recommendations, and the people behind them concede adoption will take time. Working against them are worries from end-users that any increase in notification will alienate consumers – who are now largely unaware that sensors are being used – and trigger a backlash in retail and public environments where these screens are located.

Looking ahead

Face detection has been in use for several years now, but is still very much an evolving technology. Its capabilities are steadily being enhanced to improve the overall accuracy for age brackets and genders, as well as the numbers of detectable age brackets. The technology is also being optimized to detect viewer faces from greater distances (important in larger, more open environments such as train stations and airports) and enable the sensors to cut through direct sunlight or deep shadows.

R&D work is also starting to test such new variables as the emotions of detected faces, and which way eyes are pointed when looking at a screen. Objects are also starting to be analyzed – from the accessories people may be wearing (such as hats and glasses) to the activity around viewers. The algorithms are being developed to detect and recognize brand logos, and also find and count such objects as cars, bicycles, trucks, buses, and strollers.

AVA & Privacy by Design

1. Proactive not reactive; preventative not remedial

Vendors such as Intel are providing clear and unambiguous statements about the "anonymous" nature of AVA's processes.

2. Privacy as the default

No identifiable information is collected, retained, used, or shared using AVA.

3. Privacy embedded into design

Real time video is scanned, analyzed and immediately destroyed in the AVA process.

4. Positive-sum, not zero-sum

The aggregated anonymous data provides valuable, actionable insights for users.

5. End-to-end security

Real time processing means security and privacy risks are constantly addressed.

6. Visibility and transparency

Vendors and the user community are encouraging consumer notice.

7. Respect for user privacy: keep it user-centric

Consumers should be empowered by this technology to participate and/or verify privacy claims.

There is also increasing work to drive the Return On Investment argument for these systems. AVA reporting is being blended with software-based content management systems' performance audits and Point of Sale data to develop reports on measurable consumer impacts such as sales lifts, changes in foot traffic patterns or a surge in registration numbers.

The technology is also helping gain broader acceptance, and therefore investment, into the DOOH media sector. Advertising agency planners and brand marketers are attracted by the opportunity to target consumers with TV-style advertising outside of their homes, but are also demanding network operators provide the kind of metrics most efficiently generated by automated systems such as AVA.

Granular audience counts from AVA have inspired the development of "pay per look" advertising concepts, similar to "pay per click" models used to sell online advertising. In this model, advertisers more accustomed to buying gross audience numbers could instead pay a defined fee for each face detected as actually looking at their ad.

In conclusion

Proactive efforts that not only recognize but protect consumer privacy are essential for AVA's developers and users. Using the principles of *Privacy by Design*, and the well-considered guidelines of such advocacy organizations as the DSF, as well as POPAI (Point Of Purchase Advertising Institute, which released a privacy code of conduct in 2010), will put vendors and end-users in the best position to both build and evolve the use of this technology.

Principles and guidelines are not mandates, and both vendors and end-users can embrace or ignore them. Doing the latter is the path of least resistance, however it is almost certainly the wrong choice, with the least payoff.

As the DSF noted in its guidelines: "How digital signage companies handle the privacy issues they face today will affect the way the public, regulators and advertiser clients perceive the industry – as well as the industry direction in the future." Lead with Privacy by Design, and gain a competitive advantage – your customers will thank you!

RESOURCES

Privacy by Design: www.PrivacybyDesign.ca

Center for Democracy and Technology: "Building The Digital Out of Home Privacy Infrastructure" at www.cdt.org

Digital Signage Federation Privacy Standards: www.DigitalSignageFederation.org

Recommended Code of Conduct for Consumer Tracking: www.POPAI.com

PbD

www.privacybydesign.ca

Information and Privacy Commissioner of Ontario, Canada
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca
Telephone: 416-326-3333
Fax: 416-325-9195

Intel®
2200 Mission College Blvd.
Santa Clara, CA 95054-1549
U.S.A.
Telephone: 408-765-8080
Website: www.intel.com

The information contained herein is subject to change without notice. Intel®, and IPC shall not be liable for technical or editorial errors or omissions contained herein.

April 2011

intel

Information and Privacy Comissioner,
Ontario, Canada