Face Recognition in Retail: Profit, Ethics and Privacy

Carl Gohringer, Allevate Limited

The accuracy of face recognition has increased dramatically. Though biometric technologies have typically been deployed by governments and law enforcement agencies to ensure public, transport and border safety, this improvement in accuracy has not gone unnoticed by retailers and other commercial organisations. Niche biometric companies are being snapped up by internet and social media behemoths to further their commercial interests, and retailers and other enterprises are experimenting with the technology to categorise customers, analyse trends and identify VIPs and repeat spenders. Whilst the benefits to business are clear and seductively tantalising, it has been impossible to ignore the increasing murmurs of discontent amongst the wider population. Concerns over intrusion of privacy and the constant monitoring of our daily lives threaten to tarnish the reputation of an industry which has endeavoured to deliver significant benefit to society through improved public safety. Can the industry be relied upon to self-regulate? Will commercial enterprise go too far in their quest to maximise profits? How far is too far? How can organisations ethically make use of face recognition technology to increase efficiencies and drive revenue, whilst respecting and preserving privacy and maintaining the trust of their clientele and society?

Having previously written on the subject of the application of face recognition in airports as applied by law enforcement and border control, this article looks at the increasing exploitation of the technology for commercial advantage. As well as contrasting the different use-cases defined by commercial exploitation versus public safety applications, this article also touches upon the very different agendas of those using the technology and the privacy issues that arise.

1 Advances in Face Recognition Technology

Face recognition is increasingly transforming our daily lives. A study by the US National Institute of Standards and Technology (NIST)[i] in 2010 demonstrated that the technology has improved by two orders of magnitude in accuracy over 10 years and further tests currently being conducted by NIST are expected to demonstrate its continued relentless advance. Those interested in reading of these astonishing improvements are encouraged to refer to "Advances in Face Recognition Technology and its Application in Airports[ii]", first published in Biometrics Technology Today (BTT) in July 2012, which summarises the 2010 NIST results in detail.

2 Public Safety versus Generating Profit

Most people accept that the reality of the world today necessitates certain inconveniences and intrusions. We tolerate and increasingly expect surveillance technology to be deployed wisely in situations where there is demonstrable benefit to public safety, such as at transport hubs, large gatherings, public events or areas of critical national infrastructure. The key factor behind such tolerance is comprehension; we understand the reasoning behind these uses and the benefits to ourselves, namely our safety. Though we don't necessarily like it, we generally accept it.

However, it has been difficult to avoid the increasing coverage in the media of the use of face recognition by commercial organisations. The single most common term that is bandied about in reference to these deployments tends to be "creepy". The technology being deployed is very often similar, if not identical to, the technology deployed for public safety applications. So precisely what is it about this use of technology that people are averse to?

In order to understand this, it is useful to consider in each case who people perceive benefit from the system. In the case of public safety, the people perceived to benefit are us; the citizens. In the case of commercial use, people perceive the commercial organisation deploying the technology as the beneficiaries. In this scenario the term "benefit" generally means profit, either by increasing revenues or decreasing costs. Often there is a general distrust within society of large corporations profiting from the exploitation of the populace, and this is especially true in times of prolonged economic difficulty. This is additionally complicated by the fact that our biometric traits are viewed as being something that are intrinsically ours and that are a constituent part of our definition.

3 Examples: Uses to Reduce Cost and Increase Revenue

It hasn't taken long for business minded technology companies to devise a whole range of new uses of face recognition, all focussed on delivering bottom line business benefit. An important characteristic of face recognition is that it is only useful if you have something to match a photograph (probe) against, whether it is another photograph, or a database of photographs (reference set). *It is the management, control of access to and often the creation of these reference sets that generate the most privacy concerns*.

Let us briefly discuss some of the manners in which the technology is currently being deployed.

3.1 Efficiently Identifying Customers and Staff

This perhaps is the most traditional use of biometrics within commercial organisations. The ability to positively identify people, whether they are your staff or increasingly your customers, is absolutely necessary for the day-to-day operation of business and indeed society. Biometrics can be applied to ensure identity in a more cost-effective and positive manner, thereby introducing efficiencies into the business. It is an unfortunate reality that staff are responsible for a significant amount of theft. Adopting biometric technology can eliminate password theft and help mitigate the risks of identity sharing, thereby reducing fraudulent and unauthorised transactions and ensuring relevant personnel are physically present at the time of a transaction. Additionally, customers can be identified positively before conducting transactions. Cashless payments provide numerous efficiency opportunities by allowing elimination of cash and credit cards at point of payment altogether.

3.1.1 Privacy Considerations

These examples are usually only possible with the consent and approval of the individuals in question. Customers typically register for a biometric payment system, for example, in order to realise a benefit offered by the enterprise. The enterprise in turn must satisfy the customer that their biometric reference data will be kept and managed securely and *only for the stated purpose*.

The advent of face recognition provides new manners in which you can identify your customers, for example from CCTV cameras as they enter shops or as they view public advertising displays. It is when these activities are performed without the individual's knowledge or consent that concerns arise.

3.2 Identifying Who is Entering Your Premises

These solutions are designed to integrate with existing surveillance systems; faces are extracted in real-time from a CCTV video feed and matched against a database of individuals. When the system identifies an individual of interest it can raise an alert that can be responded to rapidly and effectively, or log where and when the individual was seen for the formation of analytical data.

This can be used to provide valuable real-time or analytical intelligence to organisations, such as:

- Notification of the arrival of undesirables, such as banned individuals or known shoplifters.
- Notification of the arrival of valued or VIP customers.
- Collation of behaviour data of known customers, such as how frequently they visit, which stores they visit and integration with loyalty programmes.

3.2.1 Privacy Considerations

There are a number of potential issues with regards to privacy that need to be considered here, most notably:

- How is the reference set obtained? Who is in it?
- Do you have the permission of the individuals in the reference set?
- How are the photographs in the reference set stored and secured?
- Are the members of the reference set aware of how and when their photos will be searched?
- Are the people crossing the cameras aware that their photos are being searched against pre-defined reference sets?
- What action is taken if a probe image matches against the reference set? What are the implications of a match or a false match?
- What is done with the probe images after searching the reference set? Are they discarded or stored?

The number of possible uses of this functionality and resulting business benefits are too large to enumerate here, but very careful consideration must be made with regards to the proportionality of the solution when measured against the requirement. Additionally, the views and considerations of the individuals whose images you are verifying, both the people within the reference set and the people whose faces you are sampling as probe images, should be well understood and considered; approval should be sought for inclusion into a reference set.

3.3 Analysing How People Move Through Your Premises

Face recognition can also be used to determine how people move through premises, such as a department store. Understanding peak and quiet times is essential to enable sufficient and efficient staffing and resourcing. Raising alerts to manage unforeseen queues is critical for ensuring customer satisfaction.

Face recognition applied to CCTV can timestamp when individuals are detected at known camera locations, thereby providing highly accurate information on people flows such as:

- How long on average does it take to move between two or more points?
  (such as from the entrance of a store to a checkout or exit)
- What are the averages flow times across the day and when are the peaks?
- How does this vary with the time of day?

This can be used to determine how people typically move through the premises, and how long on average they linger in specific areas. You can also analyse this data across different age and gender demographic categories.

3.3.1 Privacy Considerations

Importantly, no person identifying information is recorded. There is no interest in identifying who the individuals moving through the premises are or in taking any specific action on any specific individual. There is no need to search against any pre-defined reference sets.

However, there are some issues you should consider when deploying such systems:

- Biometric matching of people crossing the cameras still occurs. The probe photos are matched against other anonymous people that have previously crossed the cameras.
- You should carefully consider how long this data will be retained for matching, (generally hours) and the nature of the premises being monitored.

Generally the privacy considerations of this application are minimal.

3.4 Building Databases of People Visiting Your Premises

As previously mentioned, face recognition is only useful if you have images to match against. Previous examples have dealt with matching the faces of people crossing the camera against known databases of individuals. A potentially far more valuable practice to enterprise is to dynamically build reference databases consisting of the people who cross the camera. Unfortunately, this is also the practice that riles the populace the most and is rife with potential privacy intrusions.

The increase in the use of CCTV cameras has led to an ever increasing volume of archived video footage. The intelligence in this footage typically remains inaccessible unless appropriately analysed and indexed. Such systems can be used to populate databases of "seen" individuals, thereby enabling searching for specific people of interest to determine if, when and where they have been present. This then allows the collation of data such as how frequently individuals visit your premises, how long they stay and when was the last time the individual visited your premises, as well as which of your locations any individual frequents and which is the most common.

If this functionality is combined with the ability to search and cross- reference against databases of known individuals, for example a subscribed customer database, this can then allow you to build very valuable analytical data on specific individuals thereby enabling you to predict future behaviour and market more specific services and products.

3.4.1 Privacy Considerations

Tread very carefully. Some of the most vocal opposition to the application of face recognition technology results from the capture of biometric data of potentially large numbers of people *without their knowledge or consent*, especially if the people are then identified and profiled against existing databases. In many jurisdictions around the world, the retention of such data may be in contravention of privacy legislation.

3.5 Analysing Who is Viewing What to Target Your Advertising

There have been many examples in recent months of retail and advertising organisations using technology to determine the approximate age and gender of people entering premises or viewing advertising walls. Though not technically face recognition, it is still worth mentioning here as often the distinction between the two uses is blurred. The premise is simple: such solutions can count the number of people watching an advert at any given time, and even estimate their age, dwell time, sex and race. While providing invaluable information for the advertiser, it can also allow them to dynamically change the adverts in real time to more appropriately target the demographic of the current viewer(s). Such solutions are increasingly being deployed in Japan and it is only a matter of time until they are more widely considered in Europe and North America.

3.5.1 Privacy Considerations

The key consideration here is that this form of technology is not actually identifying anybody or extracting personally identifiable information. There does appear to be some opposition to this, though none of it very vocal or serious. It is difficult to see any infringement of privacy and often may be advantageous to the consumer as advertising may be more specifically tailored to their needs.

3.6 Matching People on Your Premises with their Social Media Accounts

Both Google and Facebook have acquired face recognition technology companies over the past year. Facebook's users, for example, publish over 300 million photos onto the site every day, thereby making Facebook the owner of the largest photographic database in the world.

Facebook is already trialling a new service called Facedeals which enables its users to automatically check in at participating retail sites equipped with specially enabled cameras. In order to entice users to participate, the participating retailer can offer special deals to Facebook users when they arrive. The flow of information can be bi-directional. Such automatic check-in data coupled with the users' manual checkins can be used by Facebook to hone their profile of individuals allowing them to target users with more relevant advertising. The system is entirely voluntarily, and the reference sets searched by retailers only contain photos of users who have opted into the service.

3.6.1 Privacy Considerations

Making data from social media sites available to other commercial organisations is a potential privacy minefield and should only ever be done with users' consent. Defining these as opt-in services is exactly the right way forward. Likewise the profiling of users of social media sites based upon automatic tagging of images uploaded to those sites should be strictly controlled and only enabled on an opt-in basis. The privacy concerns over such activities have recently been very aptly illustrated by Facebook's withdrawal of its controversial auto-tagging feature from use in Europe after pressure from privacy campaigners and regulators.

4 Social Media, Cloud Computing and Face Recognition

Dr. Joseph J. Atick of the International Biometrics and Identification Association has written a thought-provoking paper entitled "Face Recognition in the Era of the Cloud and Social Media: Is it Time to Hit the Panic Button?[iii]". The paper raises several interesting points that merit mention here. In it Dr. Atick argues that the convergence of several trends including the:

- High levels of accuracy now attainable by face recognition algorithms.
- Ubiquity of social networking with its inherent large photographic databases.
- Availability of cheap computer processing and the advent of cloud computing.

…coupled with the fact that "face recognition occupies a special place [within the family of biometrics in that] it can be surreptitiously performed from a distance, without subject cooperation and works from ordinary photographs without the need for special enrolment…" is " … creating an environment … that threatens privacy on a very large scale…".

One of the main premises of the paper is that this issue "… will require the active cooperation of social media providers and the IT industry to ensure the continued protection of our reasonable expectations of privacy, without crippling use of this powerful technology".

5 Can All This Be Done Ethically? (What About Privacy?)

Can organisations ethically make use of face recognition technology to increase efficiencies and drive revenue, whilst respecting and preserving privacy and maintaining the trust of their clientele and society?

The premise of "privacy-by-design" should be used to ensure that privacy is considered from the outset of any deployment of face recognition technology. In fact, the European Union's 22-month Privacy Impact Assessment Framework (PIAF) project advises that "Privacy impact assessments should be mandatory and must engage stakeholders in the process[iv]" for all biometric projects.

Reputable organisations such as the Biometrics Institute have gone so far as to publish invaluable privacy charters [v] to act as a "…good executive guide operating over a number of jurisdictions…" which should be reviewed and seriously considered before any deployment of biometric technology.

Some of these fundamental principles are outlined below within context of the subject matter of this article and specifically within the context of commercial use of the technology. *These will not necessarily apply when discussing matters of public safety, law enforcement and national security*.

5.1 Proportionality

A fundamental principle of privacy concerns the limitation of the collection of data to that which is necessary. Organisations should not collect more personal information than they reasonably need to carry out the stated purpose. Biometric data by its very nature is sensitive and absolute assurance must be provided that it will be managed, secured and used appropriately. However, a key consideration in the use of this technology should be proportionality; is the collection of such sensitive data justified for the benefit realised?

5.2 Educate and Inform

People on the whole generally resent not being informed, especially in matters that involve them. History is littered with IT projects that have failed because key stakeholders were not involved from the outset, were not sufficiently informed and whose buy-in to the process was not obtained. Customers are one of the most important stakeholders and these issues are even more critical when dealing with their personal and biometric data.

There is a very interesting video on YouTube that illustrates this point very nicely. It is filmed by a man with a camera walking around filming random strangers without explanation. The reaction is predictably always negative and sometimes hostile. The message the video is *trying* to make is obvious: most people do not approve of being videoed, so why do we so readily accept surveillance cameras? The message that comes across is actually clearer: People object when they do not understand intent, purpose or benefit to themselves. The cameraman offered no messages of explanation of his intent, even when challenged. Objection was guaranteed.

5.3 Be Truthful and Accurate when Describing the Business Purpose and Benefit

As part of the process of informing, organisations should also be direct and open in disclosing not only the existence of the systems, but the scope, intent and purpose of the solutions. Why are you utilising an individual's biometric data? What benefit does it serve? What is the scope of the use of this data?

Importantly stay well clear of "scope creep". All too often it is tempting to start using data once you have it for other than the stated intended purpose for which it was collected. Such endeavours will inevitably lead to loss of trust.

5.4 Provide Benefit to the Customer

Simply understanding the scope, purpose and intent of a system generally will not be sufficient to garner acceptance of the system. While people are generally astute enough to realise that businesses are in the business of making money, they'll want to know what is in it for them. What is their benefit?

An example with which most of us will be familiar are grocery store loyalty or "club" cards. Whilst we all understand the objective of the grocery store is to profile and analyse our spending in order to better market to us, a majority of us still subscribe in order to receive the enticements and benefits on offer.

Within the context of face recognition, Facebook's Facedeals programme demonstrates this principle nicely. Users understand the benefit to Facebook and the retailer, yet they still may choose to opt in to the

programme because there is a clear and discernible benefit for them to do so as well, namely targeted discounts and offers at retail outlets.

This is also affirmed by a survey in 2012 by IATA[vi] which finds that "… most travellers are receptive to the idea of using biometrics within the border control process." Why? Because there is clear and discernible benefit to them in the form of a more efficient passenger process and increased levels of security.

5.5 Seek Consent and Operate on an Opt-in Principle Where Appropriate

Biometric enrolment into such systems should not be mandatory. Individuals should be allowed the ability to opt-in, with an opt-out status being the default. Clearly this is not always feasible when considering people in public places the crossing cameras. However, if they are being identified against reference sets, the individuals in the reference sets should be there only with consent. Automatic enrolment into reference sets or biometric databases should involve the consent and approval of those enrolled.

Importantly, people should not be penalised should they choose not to opt-in; they should still be allowed a mechanism of transacting and conducting their business.

The recent decision by the UK Department of Education to prohibit schools from taking pupils' fingerprints or other biometric data without gaining parents' permission is a prime example of a potential backlash when such systems are made mandatory without providing any alternative mechanism of transacting. In many cases in UK schools, students were left with no mechanism of buying their school lunch unless they enrolled into a biometric system.

6 Summary

The accuracy of face recognition has increased dramatically. Retailers and other commercial organisations are investigating ways to exploit this technology to increase revenues, improve margins and enhance efficiency. Social media companies own the largest photographic databases in existence and are under pressure from shareholders to find ways to monetise these assets. As these explorations gather pace, so does the discontent of privacy advocates.

This article has outlined a number of ways face recognition can be used by enterprise and highlights potential privacy issues. Is it possible to ethically use face recognition technology and respect privacy? This will only be possible if enterprise maintains the trust and respect of its customers. Open and honest discourse is the best manner in which to achieve this. This should be accompanied by delivering real benefit to all parties involved in a manner that also empowers the customer; nobody should be forced to enrol into biometric systems or be disenfranchised from refusing to do so.

How far is too far? History has shown that there is no absolute answer to such questions. The exact location of the line to be crossed is always a factor of and changes with the times we live in. History has also shown, especially as it pertains to technology, that it is next to impossible to put the genie back into the bottle once released. It is now the collective responsibility of all to ensure the proper and ethical use of this technology in a manner that delivers the maximum benefit. This will require the active cooperation of social media, enterprise, the IT industry and civil liberty groups to ensure the continued protection of our reasonable expectations of privacy without crippling the use of this powerful technology. In the end, the people have the loudest voice. If enterprise crosses the line, customers will pass judgement with their wallets.

7 About the Author

Carl is the founder of Allevate Limited (http://allevate.com), an independent consultancy specialising in market engagement for biometric and identification solutions. With over 20 years' experience working in the hi-technology and software industry globally, he has significant experience with identification and public safety technologies including databases, PKI and smartcards, and has spent the past 10 years enabling the deployment of biometric technologies to infrastructure projects. Carl started working with biometrics whilst employed by NEC in the UK and has subsequently supported NEC's global and public safety business internationally.

Residing in the UK, Carl was born and raised in Canada and holds a Bachelor of Science Degree on Computer Science and Mathematics from the University of Toronto.

View this article online at:
http://allevate.com/blog/index.php/2013/01/07/face-recognition-in-retail-profit-ethics-and-privacy/

Follow us on Twitter: Allevate

3,976 words

---

[i] http://biometrics.nist.gov/cs_links/face/mbe/MBE_2D_face_report_NISTIR_7709.pdf
Multiple Biometric Evaluation (2010) Report on Evaluation of 2D Still Image Face Recognition
Patrick J. Grother, George W. Quinn and P. Jonathon Phillips

[ii] http://allevate.com/blog/index.php/2012/07/17/advances-in-face-recognition-technology-and-its-application-in-airports/
Advances in Face Recognition Technology and its Application in Airports
Carl Gohringer, Allevate Limited,
July 2012

[iii] http://www.ibia.org/download/datasets/929/Atick%2012-7-2011.pdf
Face Recognition in the Era of the Cloud and Social Media: Is it Time to Hit the Panic Button?
Dr. Joseph Atick
International Biometrics and Identification Association

[iv] http://www.piafproject.eu/

[v] http://www.biometricsinstitute.org/pages/privacy-charter.html
Privacy Charter
Biometrics Institute

[vi] http://www.iata.org/publications/Documents/2012-iata-global-passenger-survey-highlights.pdf
2012 IATA GLOBAL PASSENGER SURVEY HIGHLIGHTS
The International Air Transport Association (IATA)