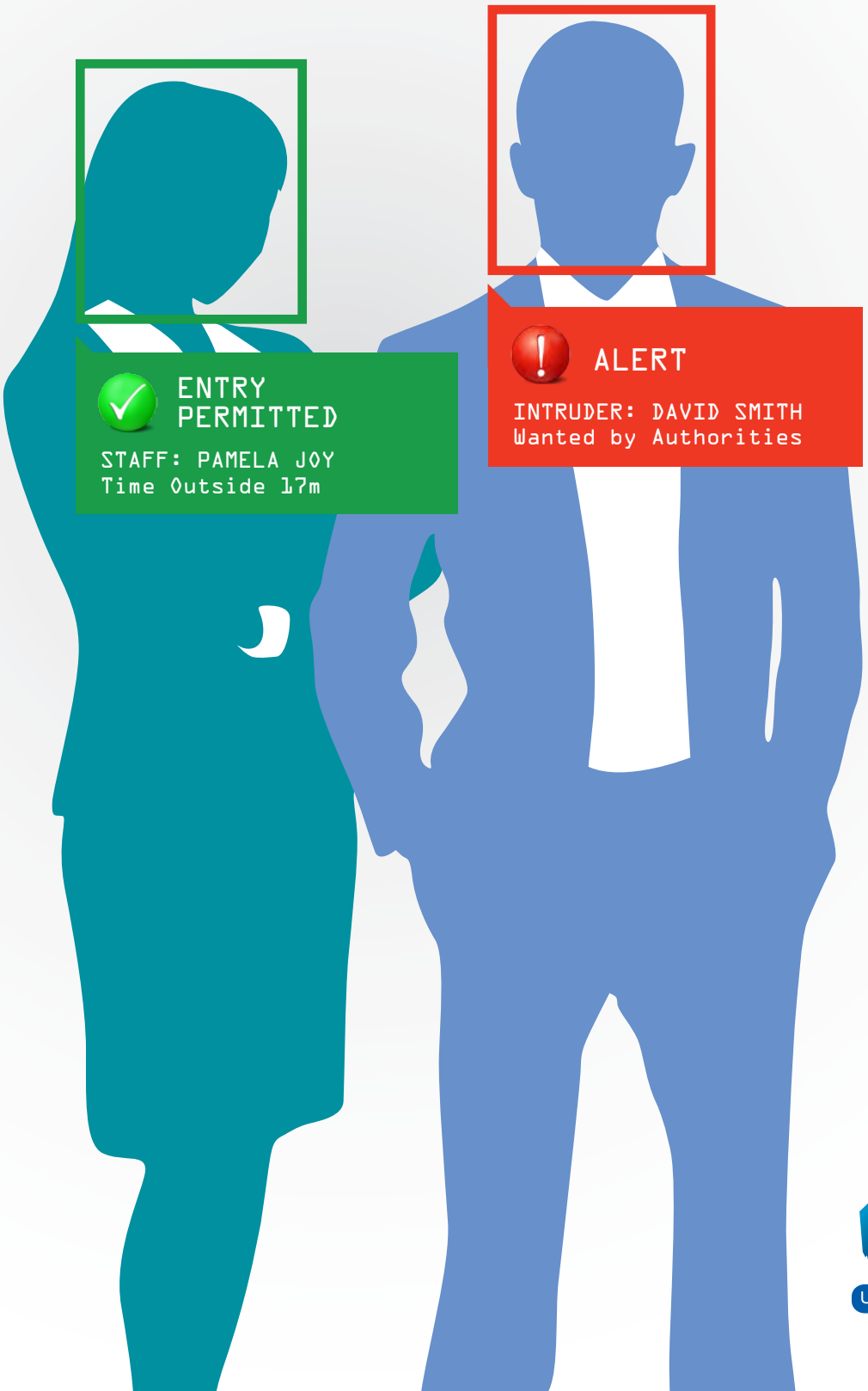
Empowered by Innovation NEC

IT'S ALL ABOUT THE FACE
FACE RECOGNITION



WE MAKE CITIES SAFER
Using technologies to safeguard lives and property

Once written off by early adopters, face recognition has come a long way to become a vital component in today's technology-driven world. This white paper explores the far-reaching effects of face recognition, and how this technology revolutionizes the security and commercial landscapes.

It's all About the Face

A face remains the most widely used way of identifying or authenticating a person. A photo of it is on most identification documents that we carry in our wallets. A lot of information can be provided from a person's face, clothing, and appearance, and today a person's face has become the epicenter of the most fascinating and promising evolving forensic technology – face recognition.

In the field of biometrics, perhaps nothing stirs up as much debate as face recognition. Using technology to identify or verify a person has always been something easily understood in theory. Heavy use of such technology in Hollywood blockbusters like *Minority Report* has certainly helped the technology gain widespread exposure among mainstream audiences. It also has to do with how naturally humans perceive one another in everyday life. We detect so many signs, say, of how a boss feels about a proposal or the type of day a spouse has had, by simply looking at the person's face.

Ironically, when a machine does that analysis, several issues come quickly to mind. For the general populace, privacy continues to be an ongoing concern. For organizations rolling out the technology, issues of accuracy and reliability continue to be a challenge.

Indeed, until recently, face recognition was far from a perfect science. While humans have always had the innate ability to recognize and distinguish between faces, computers only recently gained the same ability. The history of developing face recognition software started in the mid-1960s, when scientists began working on using computers to recognize human faces. Since then, face recognition software has progressed significantly. It is still improving rapidly today, but from the time it was first worked on in laboratories in the 1960s, the technology has advanced by leaps and bounds.

In 2006, a test of several face recognition algorithms by the National Institute of Standards and Technology (NIST) showed that machine recognition has improved tenfold since 2002 and a hundredfold since 1995. The best algorithms actually performed more accurately than most humans can manage[1].

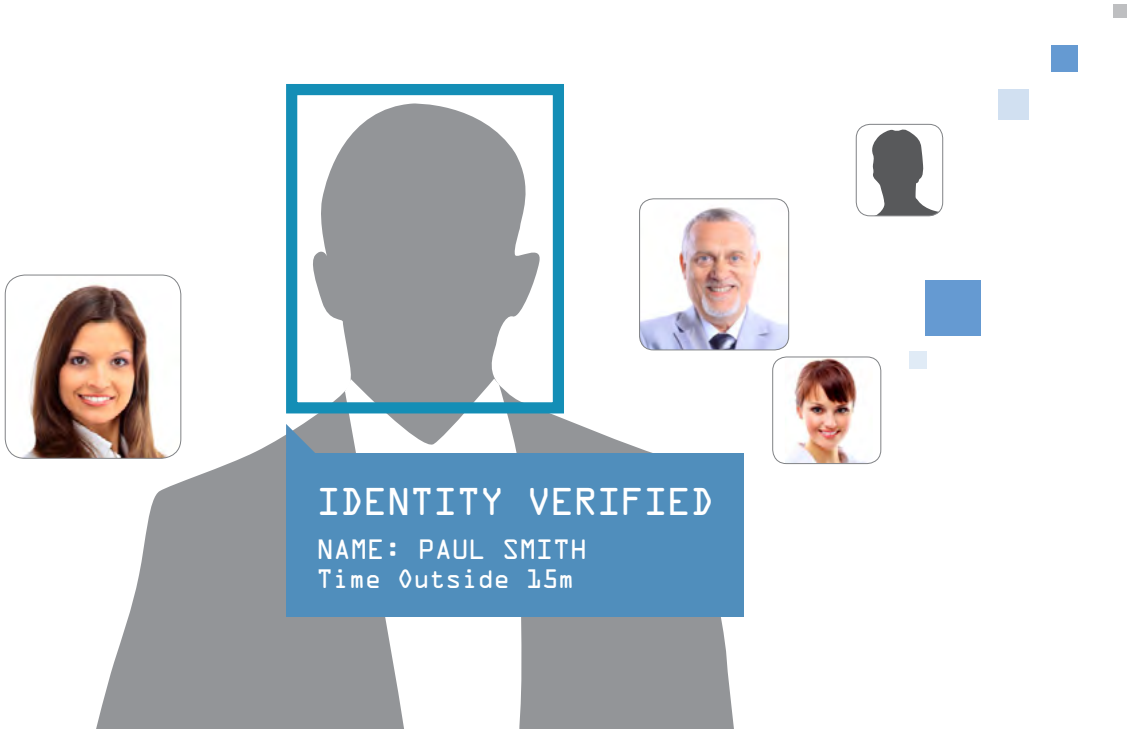
That was seven years ago. Since then, face recognition has been one of the most progressive technologies in the world, thanks in part to new methods of measuring up a face.

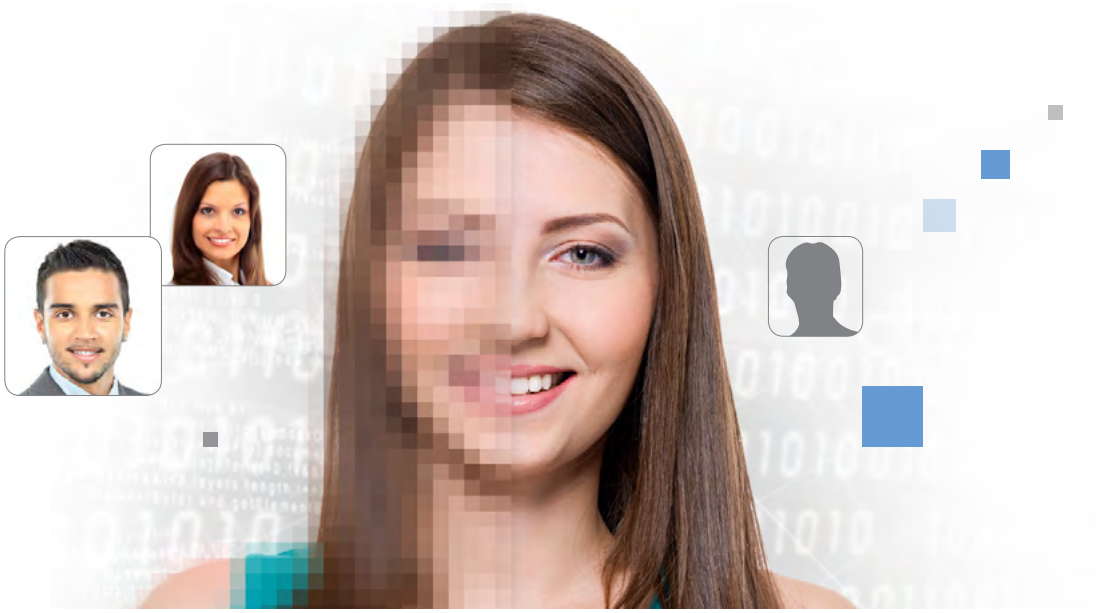
Under the Hood: How Face Recognition Works

Once it detects a face, a face recognition system determines the head's position, size, pose, and unique characteristics. Every face has numerous, distinguishable landmarks – the different peaks and valleys that make up facial features. These landmarks are called nodal points. Each human face has approximately 80 nodal points. Some of the nodal points measured by the software include:

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

The system translates nodal-point measurements into a numerical code or set of numbers, called a faceprint, representing the features on a subject's face that can be compared to faces in the database. A match is then verified from the faceprint.





Face-to-Face with the Technology

In the past, many algorithms relied on 2D measurements between a person's eyes. Despite this being a sensible method, results can be profoundly affected by the angle of view or a different facial expression. Even the smallest changes in light or orientation can reduce the effectiveness of a system, rejecting a match to any face in the database, and leading to a high rate of failure. Face recognition technology today can check on a wider number of features.

Face recognition technology now uses a 3D model and captures images in real time to select distinctive features of the face – where rigid tissue and bone are most apparent, such as the curves of the eye socket, nose and chin – to identify the subject. These areas are all unique and do not change over time. 3D face recognition can even be used in darkness and has the ability to recognize a subject at different view angles, potentially up to 90 degrees (i.e. a face in profile). 3D face analysis and skin texture comparison are just among some of the many features that have come to define the technology in recent times.

The result: more accurate matches. A more recent 2010 test by NIST reports that a person can be picked out from 1.6 million mug shots, 92 per cent of the time, by the best face recognition algorithms[2].

Indeed, if an unconstrained face recognition search had been carried out in the few days after the Boston Marathon bombings in 2013, one of the two suspects could have been correctly identified by current technologies.

The revealing findings, from two researchers from the Michigan State University, come from a series of tests using three face recognition tools available today[3]. NEC's NeoFace correctly matched one of the suspects, who was caught on camera, to a graduation photograph posted on Facebook. NEC's system pulled up the right result with both a blind search and a demographically filtered lookup, demonstrating remarkable accuracy.

The findings are also a sign of how far face recognition has come. Back in the early 2000s, several early and high-profile installations, by police and airport authorities, for example, were scaled back because of a lack of accuracy. Today, as the technology has improved, so has the acceptance.

Going Beyond Conventional Security

Previously built with the vision of improving security within the law enforcement space, the breakthrough in face recognition now sees the technology being applied within a larger audience. On top of providing enhanced security in today's post 9/11 world, the technology has proven to be versatile enough to be deployed across areas of financial services, entertainment, advertising and many more.

Banks, for example HSBC in London, use face recognition to enable authorized users to enter a secure vault[4]. This method of authentication is not only easy to use, but also highly accurate and secure.

Credit cards can also be protected by the safest, most user-friendly authentication available–the owner's face. A person paying for items at a cashier can be verified by a camera connected to a face recognition system. Pass the "face test" and the payment goes through.

Increasingly, too, companies are seeking to deploy face recognition to know customers better and provide improved service. Commercial uses, such as for customer service management, queue monitoring or business intelligence, are now benefitting from the advances in face recognition in recent years.

In London, retailers have used a face recognition solution from NEC to identify its loyal or VIP customers walking into a store. A camera picks up the image, which a computer then compares against a database. When a VIP walks in, a sales assistant is quickly alerted to provide more personalized service to him.

The scenario will remind many users of the Minority Report movie, where Tom Cruise's character walks into a retail store that instantly recognizes him from previous visits, and suggests that he could do with a Guinness.

With face recognition, targeted messages can be sent to specific individuals, instead of bombarding them with mass-produced advertisements. Ultimately, the technology serves to help match customer expectations by enabling organizations to know their customers better.

In Osaka, for example, the Universal Studios theme park uses face recognition to identify the gender and age of customers. A 60-year-old person, for example, would be greeted differently from a 25-year-old visiting the place[5].

These are but a few examples of what face recognition can offer in the coming years. With vast amounts of data collection, storage and crunching that is made available through the use of cloud technologies, it is going to provide even more insight for organizations interested in both commercial and security applications.

Here's a look at four scenarios where facial recognition may be deployed.

1 Controlling Access

Comparing a person's face with a photo ID is one of the oldest ways to verify if he can enter to a restricted place. Now, face recognition just makes that task much easier, allowing security staff at border control or even a casino to prioritize on other duties such as identifying potential offenders based on their behavior.

In Canada, the Ontario Lottery and Gaming Corporation has been turning to face recognition to automatically recognize some 15,000 self-identified problem gamblers–and keep them away from its betting tables[6].

Cameras photograph everyone who walks through the front doors of a casino, which gets 40 million visits a year. A computer then compares the images against a database of individuals who have put themselves on a self-exclusion list.

If a match is found, security guards are alerted via a silent alarm. They then carry out a manual comparison and approach for identification. If the match is confirmed, the person is escorted out of the casino.

Privacy safeguards are in place as well. The photographs of people who don't match any images on the database are discarded. Those in the database are biometrically encrypted and only decrypted when a person in one of the pictures is present.

In the same way, face recognition can be used for border control. Canada, incidentally, is also one of several countries to issue e-passports with a smart chip that can be used with face recognition technology. This allows officers, possibly in future, to compare a physical person's appearance with a digital photograph that is stored on a chip and not easily faked.

2 Finding Subjects in Law Enforcement

In the security and law enforcement sectors, the usage of face recognition is arguably the most obvious – and often accepted – to most citizens in a smart, connected city.

The technology can be used to identify, for example, known suspects who are the subject of a police investigation[7]. To do this, law enforcement agencies would have to not just collect thousands of images – both video and still images – but also to analyze the information within the tight time frame available to solve a case.

In the United States, the Federal Bureau of Investigation (FBI) is spending US$1 billion in a Next Generation Identification (NGI) program, which will add biometrics such as iris scans, DNA analysis and voice identification, along with face recognition,to an investigator's toolkit[8].

Since early 2012, a number of states have been uploading photos to a central system as part of a trial and the program is expected to be rolled out nationwide in 2014.

There are several possible use cases. Law enforcement agents might try to identify fugitives or missing persons from a face recognition database. They may also do so for unknown persons of interest. Using sophisticated multi-camera technology, they may even track subjects moving from one place to another after a critical incident.

If agents already have a suspect, they may also look out for someone they'd expect to turn up at a certain place, such as a crowded stadium. Conversely, if a riot had happened at a stadium, investigators could look at the video footage to identify who the rioters were.

The technology is already there now. The challenge is to identify subjects from a fast-growing database of photos and videos. Sometimes, face recognition is one clue in a digital trail left by a subject, for example, when he makes a call or uses a credit card.

To tap on a multi-modal database of information, many law enforcement agencies are looking to cloud-based solutions, where storage and computing capabilities are on tap should an investigation scale up.

3 Identifying Customers

A relatively new use of face recognition is in the retail space. This enables companies to quickly and seamlessly identify a frequent customer, and ensure that he or she gets personalized service without having to explicitly disclose his or her identity to the shop assistant.

A camera at the store captures images of everyone stepping inside, then sends the data to a remote computer that compares them against a database of known VIP customers. Various measurements of the face are taken and checked against a template. If a match is found, usually within a split second, the sales assistant is alerted on the smartphone or iPad to provide personalized service. He or she would also be fed details such as the customer's dress size or other preferences gleaned from previous purchases.

Already, a dozen top stores and exclusive hotels in Britain, America and Asia have been testing the face recognition technology provided by NEC. It works even when people wear sunglasses and other items that cause other face recognition technologies to stumble[9].

Because NEC uses a holistic method of combining various ways to detect a face, it works similarly to how a person would identify another. Just like how we may recognize a friend wearing glasses or with a slightly new haircut, the system is able to adapt to these subtle changes and correctly recognize a face.

4 Putting More than Just a Name to a Face

Regular customers, of course, still count. While retailers may not want to miss out on a big-spending celebrity, they will also want to make sure they understand customers providing the bread and butter sales every day.

Again, face recognition provides insights. Retailers can now "see" every single customer who walks into and uses that image data to estimate the typical gender and age of their clientele. All they need now is a camera, PC and a subscription to NEC's cloud-based face recognition service.

Leveraging on NEC servers on the Internet, the service takes images sent from a merchant and does the analysis off-site, saving merchants the heavy investments required to deploy the technology themselves. The service costs 70,000 yen (US$880) a month in Japan and has been running since its launch in 2012[10].

The use of such face recognition technology extends beyond retailers. Large malls, for example, could accurately determine the type of crowd it attracts in certain times of a day at certain parts of a complex.

The same technology could be used in interactive advertisements, which can estimate the age and gender of a person in front of them. The messages can then be customized to fit the person, resulting in a more effective pitch.

Ultimately, with intelligence gleaned from actual customers and users, retailers and advertisers can better strategize marketing plans to target the right demographic groups.

Ensuring Privacy is Protected

All the good technology cannot be used if organizations rolling out face recognition in their operations do not get the critical buy-in from users themselves.

Unlike fingerprints, it is easy to capture an image of someone's face without consent. That is a double-edged sword. Face recognition is often viewed as a "contactless" form of surveillance, identification and verification, which makes many people understandably concerned, especially about preserving their anonymity in public.

In the past year, Facebook's controversial deployment of face recognition technology to identify people in uploaded photos and even law enforcement efforts to capture and analyze publicly available images have also met with privacy concerns.

These are key issues to address should face recognition be adopted by organizations in both public and private spaces. What is important here is not just the capturing of such information, if it is in public or clearly shared by a user, but the design and governance that come with storage, access and analysis of such personal data.

The Federal Trade Commission put out a staff report in 2012, where it listed some best practices that organizations can put in place[11]. For example, companies that hold databases of consumer images should design their services with privacy in mind. Should the images be no longer needed, they should be deleted. If retained, they have to be reasonably protected.

Transparency to end users is another key point. Organizations deploying face recognition in digital signage, for example, should make clear to users that they are being observed, since they may not detect a camera in the setup.

Yet another issue brought up by the report concerns social media networks. Without a consumer's consent, they should not identify him to someone who would otherwise not be able to identify him. For example, a mobile app that lets a person identify another at a bar, with possibly added information such as his address, could raise safety risks and only be allowed with the user's consent.

Four Factors to Consider

When governments and commercial organizations decide to turn to face recognition technology, a number of questions come up often. Here are four that should be asked of a vendor proposing a solution.

1 How fast, accurate and reliable is it?

Independent tests provide a good gauge of how good a face recognition system is, and NEC has regularly come up tops in tests in the United States. In 2009, NEC's face recognition technology was ranked number one in the Multiple Biometric Grand Challenge's (MBGC) "Still Face Challenge", carried out by the National Institute of Standards and Technology (NIST) and commissioned by the United States Department of Homeland Security. In 2010, NEC again achieved the highest score in the new Multiple Biometric Evaluation or MBE 2010 benchmark.

NEC's technology is also often seen as holistic. It takes a number of methods to recognize a person, thus overcoming common issues like a unique facial expression or a pair of sunglasses blocking key features. Like how a human recognizes another, our solution uses various methods to identify a person, bypassing problems that usually fool other systems.

2 Does the face recognition require specialist, expensive cameras?

Some face recognition solutions are highly accurate only when fed high-resolution images taken by expensive, specialist cameras. This not only requires a heavy investment to cover a large area, but also makes existing cameras unusable. NEC's solution works with a diverse range of image sources, including live cameras. The resolution required for an accurate identification is also modest, making our solution a good fit in a city with various types of camera systems already in place.

3 Does the vendor provide a way to store and analyze the images on-demand, and provide the scalability in a time of urgency?

All the information in the world is useless unless it can be accessed to provide timely insights, say, during a critical event. While many vendors provide face recognition as a standalone service, NEC's face recognition solutions are part of a globally-trusted portfolio of biometric and safer cities solutions. From providing multi-modal forensics to cloud-based solutions, NEC backs up its face recognition solutions with tried and tested capabilities in related areas.

4 Is the technology open or locked in for future upgrades?

This is key to organizations looking to build a system that can be upgraded in the years ahead, as face recognition technology is improving all the time. NEC's system is flexible in the way it works with other installations. It also plugs right into our safer cities solutions, which optimize results in face recognition by making use of its findings in various related scenarios.

For more information on how face recognition can enhance your operations, contact an NEC representative at safety@gsd.jp.nec.com

References

1 http://www.technologyreview.com/news/407976/better-face-recognition-software/
2 http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968
3 http://msutoday.msu.edu/news/2013/facial-recognition-technology-proves-its-mettle/
4 http://www.tab-systems.com/wp-content/uploads/2012/12/Case_Study_HSBC_Vault.pdf
5 http://secureidnews.com/news-item/nec-taking-facial-recognition-to-hospitality/
6 http://www.theglobeandmail.com/news/national/time-to-lead/canadian-casinos-banks-police-use-facial-recognition-technology/article590998/
7 http://www.seattlepi.com/local/article/Facial-recognition-software-gives-Pierce-County-1295609.php
8 http://www.newscientist.com/article/mg21528804.200-fbi-launches-1-billion-face-recognition-project.html
9 http://www.telegraph.co.uk/technology/news/10178504/New-technology-allows-retailers-to-spot-a-celebrity-approaching.html
10 http://www.abs-cbnnews.com/business/tech-biz/11/07/12/nec-launches-new-services-facial-recognition-technology
11 http://www.ftc.gov/os/2012/10/121022facialtechrpt.pdf

Contributors

- Chris De Silva, Head of Global Face Recognition, Global Safety Division, NEC Corporation
- Paul Roberts, Face Recognition Solution Owner, Global Safety Division, NEC Corporation
- John Dowden, Law Enforcement Solution Owner, Global Safety Division, NEC Corporation

This paper is published by NEC Global Safety Division. Some of the ideas in the paper are aspirational, and NEC is working towards realizing these ideas in our vision of making cities safer.

About NEC Global Safety Division

NEC Global Safety Division, a business division within NEC Corporation, spearheads the company's public safety business globally. The Division is headquartered in Singapore and offers solutions in the following domains: Citizen Services & Immigration Control, Law Enforcement, Critical Infrastructure Management, Public Administration Services, Information Management, Emergency & Disaster Management and Inter-Agency Collaboration. Leveraging on its innovative solutions, the Division aims to help government and business make cities safer.

NEC Global Safety Division

Global headquarters: No.1 Maritime Square #12-10, HarbourFront Centre, Singapore 099253

For enquiries, please contact **safety@gsd.jp.nec.com**

nec.com/safety

WE MAKE CITIES SAFER

Using technologies to safeguard lives and property

Citizen Services & mmigration Control | Law Enforcement | Critical Infrastructure Management | Public Administration Services | Information Management | Emergency & Disaster Management | Inter-Agency Collaboration