Office of the
Privacy Commissioner
of Canada

Automated Facial Recognition

In the Public and Private Sectors

March 2013

Table of Contents

Abstract

We are not yet at the point where we can take pictures of people on the street with our smartphones, identify them, and gain access to information about them. However, this reality may not be too far off and we can only imagine what that will do to our interactions, relationships, and how we conduct our lives. For one thing, this will exacerbate the economic and social divide between those who have access to the technology and those who do not. It will also make surveillance and facial recognition seem ordinary. If the use of this technology is normalized, no one will question it and put constraints around what it can be used for and by whom.

Introduction

The Office of the Privacy Commissioner of Canada (OPC) has kept track of developments in facial recognition for many years in the context of our broader interest in biometrics. Nearly a decade ago, we identified facial recognition as having the potential to be the most highly invasive of the current popular biometric identifying technologies, since the subject doesn't need to give consent or even participate knowingly.

Automated facial recognition involves the identification of an individual based on his or her facial geometry. For facial recognition to be successful, there needs to be a quality digital image of an individual's face, a database of digital images of identified individuals, and facial recognition software that will accurately find a match between the two.

Of all biometric technologies, facial recognition most closely mimics how people identify others: by scrutinizing their face. What is an effortless skill in humans has proven immensely difficult and expensive to replicate in machines. But through a convergence of factors in the past few years, facial recognition has become a viable and increasingly accurate technology.

Digital images have become pervasive, through the proliferation of surveillance cameras, camera-equipped smart phones, and inexpensive high-quality digital cameras. Cheap data storage has led to massive online databases of images of identified individuals, such as licensed drivers, passport holders, employee IDs and convicted criminals. Individuals have embraced online photo sharing and photo tagging on platforms such as Facebook, Instagram, Picasa and Flickr. There have also been significant improvements in facial recognition technology, including advancements in analyzing images and extracting data.

Faces have been transformed into electronic information that can be aggregated, analyzed and categorized in unprecedented ways. What makes facial image data so valuable, and so sensitive, is that it is a uniquely measurable characteristic of our body and a key to our identity.

Some security applications of facial recognition technology are undoubtedly beneficial, such as authentication of employees allowed to access nuclear plant facilities, for example. At the same time, facial recognition holds implications for privacy and for societal values in general. Some commentators[1] have even concluded that facial recognition technology could spell the end of anonymity.

This research paper aims to explain in simple terms how facial recognition technology works, examine some applications in the public and private sectors, and discuss the privacy implications.

What is facial recognition?

a) Overview

Facial recognition technology aims to identify or authenticate individuals by comparing their face against a database of known faces and looking for a match. The process can be broken down into 3 very general steps. First, the computer must find the face in the image. It then creates a numeric representation of the face based on the relative position, size and shape of facial features. Finally, this numeric "map" of the face in the image is compared to database images of identified faces, for example, a driver's license database.

Facial recognition can be used to either confirm or discover someone's identity. Authentication type systems are used to grant access to facilities or equipment. Other uses include combating fraud, for example, checking whether an individual has submitted a passport application under more than one name. Other types of biometrics are currently being used for authentication, such as the use of fingerprints and iris scans.

Identification is often the goal of public safety and national security applications, such as identifying individuals during a riot, or maintaining the security of high traffic public places such as airports and sports arenas. Facial recognition is highly suitable for identification applications because facial images can be captured at a distance and without the individual's knowledge. Other biometrics, like gait or voice recognition, can also be used for identification from a distance and without consent, but they have obvious limitations that render them less useful.

b) Accuracy

A number of factors influence the accuracy of facial recognition technology:

- the system can only recognize individuals whose images are in the database;
- images must be of sufficient quality in order to be used reliably;
- the system has a sensitivity threshold that must be set appropriately so that there are not too many false positives (wrong person is identified) or false negatives (a person who should have been identified is not); and,
- lighting, glasses, facial hair, makeup, and angle from which the photos are taken.

A recent innovation in facial recognition has been the use of 3D images, which capture information about the shape of the subject's skull. This makes the system less vulnerable to lighting issues and allows for the matching of images taken from different angles.

In 2010, the U.S National Institute of Standards and Technology tested[2] various facial recognition systems and found that the best algorithm correctly recognized 92 percent of unknown individuals from a database of 1.6 million criminal records.

A 2011 study[3] from Carnegie Mellon University showed that facial recognition technology could be used to identify individuals in the real world from personal online images. Researchers were able to identify strangers and find their personal information using facial recognition software and social media profiles.

- In one experiment, the researchers used publicly available images from online social network profiles to identify individuals on a popular online dating site where members use pseudonyms. One out of 10 of the dating site members were identifiable.
- In a second experiment, the researchers were able to identify 31% of students walking on campus using their profile photos on Facebook.
- In a third experiment, the researchers predicted personal interests and, in 27% of cases the first 5 digits of students' Social Security numbers, based on a photo of their face.

The study demonstrated that an individual's face can be used to link his or her online and offline identities without any special database access. Although the researchers concluded that face recognition of everyone, everywhere, all the time, was not yet feasible due to technological limitations (accuracy) and computational costs, they believe that those limitations will fade over time.

c) How is face detection different from facial recognition?

Face detection is the process of finding a face in an image and involves less precision than facial recognition. No individual-level matching occurs with an identified image.

Face detection has been used in commercial applications for a number of years. For example, this technology is used in digital signs to detect the gender, age and emotion from facial expressions of passers-by for the purpose of delivering targeted advertising.

It is conceivable that in the future, digital signs will be capable of identifying consumers by matching their faces with online image databases, such as social network profiles, in order to deliver more accurately targeted ads. The U.S. Federal Trade Commission speculates[4] that stores might start collecting consumer photographs as part of their loyalty programs in order to be able to target consumers with offers based on their interests and movements.

SceneTap is a mobile application that uses cameras and facial detection software to monitor the general demographic makeup of crowds in bars and clubs. The app is used to find out the average age and gender ratio of patrons to help potential patrons decide which venue to go to. The information is also useful to marketers wanting to reach a particular demographic without identifying specific individuals.

As with digital signage, however, SceneTap may potentially become more intrusive in future. In June 2012, the company filed a patent application[5] that describes the collection of much more detailed information, such as race, height, weight, attractiveness, hair color, clothing type, and the presence of facial hair or glasses. If enough information about individuals is collected, this may lead to individuals being identified, thus triggering much more serious privacy concerns.

The Microsoft Kinect gaming platform is able to identify users and bases its advertising platform on being able to tell who is in the room, how old they are and whether they are engaged with what is happening on the screen. Similar sensors are part of some TVs sold today, and can be used to find out a viewer's reactions to a TV show or movie[6].

Public sector applications of facial recognition

Since facial recognition technology was first conceived as a tool for government security and law enforcement, it is not surprising that it is primarily used by the public sector. It is worth noting that the public sector also runs most databases of identified individuals, such as driver's licence holders, passport holders and convicted criminals.

Law enforcement and national security

The day after the June 2011 hockey riot in Vancouver, the Insurance Corporation of British Columbia (ICBC) offered to help police identify rioters by running facial recognition software on images from the riot and comparing suspects to images in its drivers licence database. The BC Privacy Commissioner ruled that while ICBC can use the technology to detect and prevent driver's licence fraud, the corporation cannot use its database to help police identify riot suspects because this is a different purpose, of which customers were not notified[7].

These events led to the tabling of a federal Private Members Bill, Bill 309, An Act to Amend the Criminal Code (Concealment of Identity) that proposed to criminalize the wearing of masks during unlawful protests. Concerns have been expressed[8] that the new law (which received Royal Assent June 19, 2013) would create a chill on protests, including peaceful ones.

In the U.S., FBI's Next Generation Identification Program (NGI) uses a variety of biometrics, including facial recognition, to identify and monitor "persons of interest." For the facial recognition component of the program, which is expected to be fully operational in summer 2014[9], the FBI will integrate its own databases of searchable photos with those at the state level. The resulting database will contain the biometric and biographical information of over 100 million Americans; will be integrated with the extensive networks of CCTV cameras that already monitor public and commercial spaces, such as streets, parking lots, airports, banks, and shopping malls; and will be made available to different levels of government.

Border security

As part of the perimeter security initiative, Canada and the U.S. have discussed using face recognition scanners linked to image databases in both countries. The purpose would be to identify wanted individuals or convicted criminals[10].

In Australia, facial recognition is used in conjunction with fingerprinting at borders to identify fraudulent visa applicants[11]. Australian immigration officials are also using facial recognition in efforts to address visa fraud and illegal workers[12]. This is part of a national campaign to crack down on identity theft and the use of false identities to facilitate crime.

Japan is testing automated immigration gates at its major airports whereby the faces of inbound and outbound travelers are automatically compared to their passport pictures. This is intended to speed traveler traffic through immigration gates[13].

Drivers' licences

Drivers' licences in many Canadian provinces, such as Ontario, BC, and Manitoba, include facial recognition-ready photographs. Facial recognition is used during the licence application process to detect id theft and fraud, for such purpose as identifying individuals who apply under different names.

Casinos

Facial recognition is used in many Canadian casinos in order to detect known criminals and cheats. Also, as part of voluntary self-exclusion programs in several provinces, including Ontario and British Columbia, facial recognition is used in province-run casinos to keep out individuals who have asked casinos to deny them entry in order to stave off gambling addictions, for example.

Cameras in Ontario casinos run facial recognition software on individuals entering the building and compare images with a database of self-identified gamblers who ask to be placed on a no-gambling list. The program is entirely voluntary and works to recognize only individuals who have provided explicit consent. The Ontario Privacy Commissioner approved[14] the program because of its privacy-enhancing design. Images which do not have a match with the gambler database are discarded. Also, the gambler database is secured using biometric encryption, whereby information specific to an individual can only be unlocked when that individual is physically present.

Drones

Drones are increasingly being used by law enforcement and government agencies in Canada and internationally. In the U.S., there will be as many as 30,000 drones by the end of this decade[15], with implications for Canada along the border. According to a 2013 U.S. Congressional Research Service report, "In the near future, law enforcement organizations might seek to outfit drones with facial recognition or soft biometric recognition, which can recognize and track individuals based on attributes such as height, age, gender, and skin color… and will soon have the capacity to see through walls and ceilings."[16] An OPC research report entitled "Drones in Canada" addresses the privacy implications of drones in more detail.

Military applications

The U.S. Navy has reportedly been using Robocop-style glasses, which are fitted with a small camera that sees as far as 19 km. The glasses can capture 400 images a second and compare them with a central computer database of 13 million faces[17].

Technology being considered by the U.S. military consists of a camera integrated with a soldier's optics for his weapon, together with a portable database that could contain over a million images. This equipment would allow soldiers to identify terrorists and other enemies in seconds in the field without requiring any bandwidth[18].

Another potential military application involves robots equipped with facial recognition software that would be sent into the field to retrieve wounded soldiers[19].

Sporting events

Facial recognition technology is increasingly a part of security measures at large sporting events. At the China Olympics in 2008, all those entering the main stadium underwent identity checks at facial recognition checkpoints[20]. Facial recognition was also used in London for the 2012 Olympic games to keep watch for identified suspects.

At the 2014 Soccer World Cup, Brazilian police plan to use Robo-cop style glasses with facial recognition capabilities to scan the crowd and identify potential troublemakers. According to reports[21], a camera in the glasses will capture up to 400 facial images per second, and compare biometric markers with a database of 13 million known criminals. The camera can apparently be used to identify individuals up to 50 metres away.

Facial recognition and the *Privacy Act*

To date, the use of facial recognition technology by Canadian federal government departments and agencies has been limited. At the time of publishing this research report, the OPC has not received any complaints under the Privacy Act involving facial recognition. However, we have addressed the issue in the context of the Privacy Impact Assessment (PIA) process.

a) Privacy Impact Assessments

Since 2004, the OPC has been reviewing PIAs for Passport Canada's Facial Recognition Project, which uses facial recognition technology to detect fraud among passport applicants. An applicant's photo is matched against the Passport Canada photo database to determine irregularities, such as whether the same individual is applying for passports in different names.

Throughout the implementation of the project, the OPC has made a number of recommendations and suggestions to Passport Canada to mitigate the privacy risks of this program, and many of these have been implemented. In 2012, the OPC had the following recommendations:

- Record a summary of the biometric data rather than the image itself to reduce the likelihood of biometric data being used for a different purpose that may be unauthorized;
- Store biometric information locally rather than in centrally located databases to minimize the risk of data loss or inappropriate cross-linking of data across systems; and
- Use biometric data to *authenticate* the identity of individuals, which involves the matching of one biometric sample to one sample on record. Avoid using biometric data to *identify* individuals, which involves matching one biometric sample against all records in a database. One-to-one matching reduces the risk of false matches and data breaches.

As facial recognition technology is further developed, opportunities to incorporate it into federal surveillance programs could increase. For example facial recognition technology could be added to existing video surveillance systems, such as those used by the RCMP on Parliament Hill, the Canadian Air Transport Security Authority in airports, and by the Canadian Border Services Agency at all border crossings. The OPC continues to encourage federal institutions to consult with us about their plans to use facial recognition technologies in the future.

b) Assessing need

Generally speaking, any federal institution collecting personal information can only do so if the information relates directly to an operating program or activity of the institution. The OPC would encourage any institution contemplating the use of facial recognition to ensure that it can clearly justify the prospective privacy intrusion. To guide this analysis, institutions can use the following four-part test:

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Would the loss of privacy be proportionate to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?

c) Consistent use

Another privacy concern is the potential for cross-matching, whereby a face print collected for one purpose would be used without a person's consent for a different purpose. Under the Privacy Act, federal government institutions can use personal information for the purpose for which the information was collected or for a use consistent with that purpose. Apart from some limited and specific exceptions, the consent of the individual must be obtained for any other use of the information. Because face prints are unique identifiers, there may be a temptation to use them beyond their original stated purpose, and to match information across databases. For example, data collected for immigration purposes by one department might be inappropriately used for national-security purposes by a different government agency. The matching of information across databases can also lead to the creation of enhanced profiles of individuals.

d) Access and retention

Another privacy challenge is the storage of facial image information in databases and the need for strict access controls. Of particular concern in the sharing of information with other agencies and governments, including law enforcement, with the risk of government tracking and surveillance without appropriate authorization, safeguards or oversight. Moreover, federal government departments and agencies should implement and respect strict retention policies and dispose of the information once it is no longer required.

e) OPC Guidance on biometrics

In 2011, the OPC issued guidance on the use of biometrics such as facial recognition in both the public and private sectors. The document, entitled "At Your Fingertips – Biometrics and the Challenges to Privacy", proposes several principles aimed at mitigating privacy challenges associated with biometric systems, including:

- Record a summary of the biometric data rather than the image itself to reduce the likelihood of biometric data being used for a different purpose that may be unauthorized;
- Store biometric information locally rather than in centrally located databases to minimize the risk of data loss or inappropriate cross-linking of data across systems; and
- Use biometric data to *authenticate* the identity of individuals, which involves the matching of one biometric sample to one sample on record. Avoid using biometric data to *identify* individuals, which involves matching one biometric sample against all records in a database. One-to-one matching reduces the risk of false matches and data breaches.

Private sector applications of facial recognition

Commercial applications of facial recognition began appearing on the market late last decade. In 2008, for example, Lenovo released a line of laptops that allowed users to log on using their face instead of a password. As these devices become more sophisticated, their price is dropping. For example, the video surveillance manufacturer Gadspot announced[22] that it will be selling, for under $150, "intelligent" security cameras with built-in facial recognition.

a) Online services

A number of online companies use facial recognition as part of services or features. Facebook, Apple and Google all use facial recognition to assist in tagging images with individuals' names.

Facebook's image database is likely the largest in the world. By mid-2011, an estimated 100 billion photos had been uploaded to Facebook and approximately 250 million photos are being uploaded every day[23]. Of significant privacy concern is the fact that Facebook has the ability to combine facial biometric data with extensive information about users, including biographic data, location data, and associations with "friends." Since Facebook has approximately 1 billion users to date, this would potentially make Facebook the holder of the most comprehensive profiles on a large segment of the world population. In fact, the New Yorker has called Facebook "a directory of the world's people.[24]"

Examples of other online services that use facial recognition are:

- Dailymakeover[25] - a website that allows women to upload their image and try on different makeup, clothes, and hairstyles.
- FindYour FaceMate[26] – a dating site that matches individuals based on similar facial features.
- Doggelganger[27] – a service sponsored by Pedigree to promote dog adoption. Facial recognition software matches images of prospective dog owners with dogs that look like them.

b) Mobile security

Security experts are increasingly promoting the use of human attributes to allow access to mobile devices. The premise is that mobile devices are vulnerable to theft and loss, and the use of biometrics to unlock the device will make it less likely that data on the device will be accessed. Passcodes and passwords are increasingly shown to be ineffective, in part because people are not very creative in choosing them.

On mobile devices, the challenge has been to have a high-quality camera and a powerful processor capable of carrying out the complex algorithms needed for facial recognition while limiting power consumption. With technological advancements, these issues are being solved.

Both Android and Apple smartphones support facial recognition technology. The phone's camera scans the owner's face and compares it with an image created by the owner. If there is a match, the phone will unlock. In 2012, 20% of all smartphones shipped had facial recognition capability. It is estimated that within five years, 665 million smartphones and tablets will include facial recognition[28].

c) Home security

Facial detection and recognition systems are also being used for security purposes in the offline world. Gadspot, mentioned earlier, manufactures inexpensive facial recognition enabled security cameras. An Ottawa company, iWatchLife, sells smart surveillance cameras that can alert home and business owners to certain events, such as if the number of individuals on the premises exceeds a set amount. The company is working[29] to add a facial recognition component that could be used for features such as access control, for example, not allowing a service person to enter a home office.

d) Retail and banking applications

A US company[30] is marketing facial recognition software that can be integrated with ATMs and retail point-of-sale terminals to provide secure authentication. The software is designed to work with existing security cameras.

An Italian company developed the EyeSee mannequin that uses a camera disguised as an eye to collect data such as age, gender and race about passing shoppers. While to date, only face detection technology is being used, facial recognition applications[31] may not be far off.

Also in the retail sector, NEC has launched a facial recognition service that collects not only demographic data about shoppers, but also their shopping habits, such as frequency and timing of their visits.

e) TV

Facial recognition has been incorporated into smart TVs by brands like LG, Samsung and Panasonic. The TV set offers menus of shows or online media based on who is watching. The media rating company Nielsen is exploring the use of smart TVs for measuring ratings and getting a better idea of who is watching shows and ads[32].

Facial Recognition and PIPEDA

At the time of publishing this research report, the OPC had not received any complaints under *The Personal Information Protection and Electronic Documents Act* (PIPEDA) involving facial recognition. Facial recognition would likely trigger the application of PIPEDA when used by organizations in the course of a commercial activity. The principles that are key in any examination of the use of facial recognition by private sector organizations are discussed below.

a) Appropriate purposes

The uses of facial recognition range from seemingly benign, like authentication on a laptop or access to restricted areas, to potentially creepy, like being identified when walking into a store. When faced with technology that pushes the boundaries of possibility, it can be a challenge to decide which applications are those which a reasonable person would consider to be appropriate in the circumstances and those which are not. The four-point test that the OPC uses under the Privacy Act to evaluate the appropriateness of using facial recognition for the stated purpose is also applied under PIPEDA. For an in-depth discussion, please refer to OPC's guidance piece on biometrics, entitled "Data at Your Fingertips."

b) Consent

Under PIPEDA, an organization must inform individuals of all the uses of their personal information in order for their consent to be considered meaningful. As technological capabilities become more diverse and the range of potential secondary uses expands, it may prove to be a challenge for organizations to meaningfully convey to individuals what their image will be used for and by whom. An added wrinkle is the challenge of obtaining meaningful consent in a mobile environment. Since facial recognition can be carried out surreptitiously without individuals' knowledge and consent, it may sometimes prove tempting for organizations to simply not inform individuals and individuals would have no way of knowing how their personal information is being used.

c) Safeguards

PIPEDA requires that security safeguards be appropriate to the sensitivity of information. Facial image data is particularly sensitive because it is unique and can be linked to many other individual-level data. If there is a

data breach, individuals will be much more at risk of identity theft because biometrics cannot be changed like a password. Thus, organizations must take strict security precautions when storing facial recognition information.

d) Accuracy

False matches continue to be a problem as facial recognition technology is still far from being foolproof, particularly in uncontrolled situations. Such errors could have serious implications for individuals, for example, if their information becomes intertwined with someone else's.

Other International Enforcement Developments

The OPC is not alone in its efforts to set appropriate parameters around the deployment of facial recognition technologies.

The EU Article 29 Data Protection Working Party issued an opinion[33] on facial recognition in online and mobile services in March 2012 with the aim of considering the appropriate legal framework and providing recommendations to address a range of data protection concerns. The risks to privacy identified include lack of consent, insufficient safeguards, and lack of individual access. The opinion concluded that facial recognition technology could spell an end to anonymity.

In April 2012 the Working Party issued an opinion[34] on developments in biometric technologies which states that consent must be obtained for the storage and use of biometric data.

On October 15, 2012, Facebook disabled its tagging facial recognition feature for users in the European Union, following an investigation by the Irish DPA. The Hamburg DPA also declared that Facebook was in violation of the EU's data protection laws with regard to its use of facial recognition and took measures to force Facebook to amend its practices as well as destroy its data base of facial images collected in Germany to date[35].

In the fall of 2011, the OPC hosted a meeting with members of the Article 29 Working Party to discuss the privacy implications of facial recognition. Among the topics discussed was digital signage and Facebook's tag suggestion feature.

The potential of facial recognition technologies to end anonymity is also of concern to the Federal Trade Commission (FTC). In October 2012, the FTC released best practices[36] aimed at companies that use facial detection and facial recognition technologies. The FTC recommends that companies should obtain express consent from consumers when they are using facial recognition to identify someone who would otherwise be anonymous. As well, express consent is also recommended when facial recognition data is used for a different purpose than stated at the time of collection.

In Britain, the Surveillance Commissioner has warned[37] that high-definition CCTV cameras that facilitate increasingly accurate image analysis, including facial recognition, are being rolled out across the country, endangering privacy and other civil rights. He has called for regulation in both the public and private sectors.

Conclusion

Our ability to remain anonymous both online and off is diminishing with each passing day. Information about our activities is captured in minute detail by technologies that we have willingly incorporated into our daily lives, as well as technologies we cannot escape. Third parties use this data to analyze, sort, categorize and increasingly identify us: government and law enforcement use it to maintain public safety and national security, and commercial interests use it to maximize profits. Our online activities are increasingly tied to our real identities, and third parties are striving to make links between our online and offline selves. We ourselves collude in this tracking activity as we go about our daily lives tethered to our smartphones, uploading information about ourselves and those around us.

Facial recognition does not seem so far-fetched in this ecosystem. The pace of technological advancement as well as its uptake by individuals has been incredibly rapid in the last decade. Researchers and policy makers are only beginning to catch up in considering the societal implications of this road we are collectively on. What will it mean if we can no longer be anonymous?

In his essay "The Virtues of Anonymity[38]," Daniel Solove wrote:

Given the dark slimy things that crawl underneath the cloak of anonymity, one's first instinct might be to celebrate when modern technologies destroy anonymity…But the destruction of anonymity is not necessarily a good thing. For all its vices, anonymity has many virtues. With anonymity, people can be free to express unpopular ideas and be critical of people in power without risking retaliation or opprobrium. The anonymity in everyday life enables people to be free to do many worthwhile things without feeling inhibited.

Facial recognition makes real a futuristic scenario where people can be photographed with or without their knowledge and identified using online databases. Their name can then be combined with other information on social media sites, Internet search records and other sources. This information can include contact information, bank and credit card data, credit scores, travel patterns, shopper profiles, interests and opinions. In other words, by using facial images and online data, detailed profiles can be quickly compiled by individuals, commercial interests and government authorities.

It is difficult to talk about the effects of facial recognition without talking about the effects of surveillance. Facial recognition brings a new dimension to surveillance in that it makes it much easier to identify individuals in a very short period of time. Its integration with data mining will also allow for automated tracking of individuals in the real world, and will tie online and offline activities.

Ian Kerr and jennifer barrigar, in considering the relationship between privacy, identity and anonymity in our increasingly networked society, said,

> *The ability or inability to maintain privacy, construct our own identities, control the use of our identifiers, decide for ourselves what is known about us, and, in some cases, disconnect our actions from our identifiers will ultimately have profound implications for individual and group behaviour. It will affect the extent to which people, corporations and governments will choose to engage in global electronic commerce, social media and other important features of the network society. It will affect how we think of ourselves, the way that we choose to express ourselves, how we make moral decisions, and our willingness and ability to fully participate in political processes.*[39]

Undoubtedly, facial recognition holds great promise for public safety and security. Law enforcement agencies, for example, can tap into facial image databases, both public and private, in the course of investigating

suspected criminal activity. However, facial recognition also poses grave risks for democracy and society if it is allowed to be used indiscriminately, by anyone for any purpose. Likely, there will be effects on freedom and autonomy, people's capacity to act and make decisions based on their own values and beliefs. People may be motivated by fear of reprisal, and fear of standing out from the crowd. Neil Richards, in his paper[40] on the dangers of surveillance, states, "Surveillance is harmful because it can chill the exercise of our civil liberties and because it gives the watcher power over the watched." In the case of facial recognition, power lies in the fact that the watched are being identified sometimes unknowingly while the watchers are generally anonymous, and often invisible.

From a technical perspective, facial recognition systems generate better results for certain demographic groups over others[41]. If these systems were to have better recognition rates for distinct groups, this could lead to disproportionate scrutiny, and possibly racial profiling and discrimination. Too many false negatives also pose a concern since this would promote a false sense of security that the system is more effective than it is in reality.

The availability of cheap facial recognition for the masses may have the effect of normalizing surveillance over time. We are not yet at the point where we can take pictures of people on the street with our smartphones, identify them, and gain access to information about them. However, this reality may not be too far off and we can only imagine what that will do to our interactions, relationships, and how we conduct our lives. For one thing, this will exacerbate the economic and social divide between those who have access to the technology and those who do not. It will also make surveillance and facial recognition seem so ordinary that no one will question it and put constraints around what it can be used for and by whom.

For now, many may be accepting of facial recognition being used for public safety and security purposes. The fear is, however, that the technology will be misused to further other goals of governments, such as clamping down on dissent. There is also worry about how well the biometric data is safeguarded and how vulnerable it might be to hacking and malicious misuse in the wrong hands. The proliferation of potential uses by private sector organizations driven by strong incentives for commercial gain is also cause for concern.

In our society, individuals can decide, in most online and offline circumstances, when to disclose their identity to others. However, with the increasing power of others to identify previously anonymous individuals without knowledge or consent, our control over our sense of identity will irreparably erode -- in both the physical and virtual worlds. With the proliferation of data brokers as well as data sharing agreements between governments, we may not even be aware of who has access to our personal information or what personal information is being associated with our identities. Given these implications, strict controls and increased transparency are needed to ensure that the use of facial recognition conforms with our privacy laws and our common sense of what is socially acceptable.

References

Nelson, Lisa S. *America Identified: Biometric Technology and Society*. The MIT Press, 2011.

Pugliese, J. *Biometrics: Bodies, Technologies,* Biopolitics. Routlage. 2010

Gates, Kelly A. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.* New York University Press, 2011.

LI, Stan Z. and Jain, Anil K. *Handbook of Facial Recognition*. Springer, 2011.

Pepper, Scott R."Unraveling Privacy: The Personal Prospectus & the threat of a Full Disclosure Future" Northwestern University Law Review, 2011.

Acquisti, A, Gross, R. and Stutzman, F. "Faces of Facebook: Privacy in the Age of Augmented Reality." Presentation at the Black Hat USA 2011 conference.

Endnotes

[1] Hao Li, "Germany wants to halt Facebook facial recognition," International Business Times, Aug 4, 2011.
[2] Patrick J. Grother, George W. Quinn and P. Jonathon Phillips, *Report on the Evaluation of 2D Still-Image Recognition Algorithms*, of Standards National Institute of Standards and Technology, August 24, 2011.

[3] Alessandro Acquisti and Ralph Gross, *Faces of Facebook: Privacy in the Age of Augmented Reality*, Carnegie Mellon University, July 2011.
[4] *Protecting consumer privacy in an era of rapid change*. Federal Trade Commission Staff Report, March 2012.
[5] Kashmir Hill, "SceneTap Wants to One Day to Tell You The Heights, Weights, Races and Income Levels Of The Crowd At Every Bar," Forbes, Sept 25, 2012.
[6] Tarun Wadhwa, "*What Do Jell-O, Kraft And Adidas Have In Common? They All Want To Know Your Face*,"Forbes, Aug 8, 2012.
[7] Office of the British Columbia Privacy and Commissioner, "*Investigation Report F12-01: Investigation into the use of facial recognition technology by the Insurance Corporation of British Columbia*," Feb 16, 2012.
[8] Patrick White, "*New bill refines rules on masks in unlawful protests*," The Globe and Mail, Nov 1, 2012.
[9] Jerome M. Pender, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law*, Federal Bureau of Investigation, July 18, 2012.
[10]"*Border workers push for biometric screening in perimeter security plan with U.S.*," Secure ID News, June 1, 2011.
[11] Samantha Maiden, "*Biometric security at borders to catch visa fraud*," The Sunday Telegraph, April 1, 2012.
[12] Ray Clancy, "*Facial recognition software being used in Australia to track down visa fraud*," Australia Forum.com, Feb 7, 2013.
[13] "*Test of facial ID recognition system begins at airports*," The Asahi Shimbun, Aug 7, 2012.
[14] "*OLG and Commissioner Cavoukian announce state-of-the-art Privacy-Protective Facial Recognition System*," PrivacybyDesign. Nov 12, 2010.
[15] Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, Congressional Research Service, April 3, 2013.
[16] *Ibid.*
[17] http://www.cbc.ca/news/canada/british-columbia/story/2011/06/18/bc-icbc-rioters-id.html
[18] Martin Barillas, "*New military applications for facial recognition technology*," Spero News, Sept 2, 2012.
[19] "New first responder," University of Dayton site, Aug 24, 2012.
[20] "*Facial recognition technology safeguards Beijing Olympics*", Chinese Academy of Sciences site, Aug 15, 2008.
[21] Jan Corpus, "*2014 World Cup Will Test Robocop Facial Recognition Technology*," Bit Rebels.
[22] Stephen Mayhew, "*Gadspot to sell security cameras with facial recognition in North America*," Biometric Update, Oct 10, 2012.
[23] "*How much do you know about Facebook photos*?" Pixable blog, February 14, 2011.
[24] Jose Antonio Vargas, "*The Face of Facebook*," The New Yorker, September 20, 2010.
[25] http://www.dailymakeover.com
[26] http://findyourfacemate.appspot.com/
[27] http://www.ourshowroom.co.nz/doggelganger/
[28] Joel Rai, "*In your face*," Business Today, Aug 5, 2012.
[29] Ivor Tossel, "Facial-recognition technology needs limits, privacy advocates warn," The Globe and Mail, Sept 26, 2012.
[30] "*O2 Secure Wireless intros facial recognition integration software for ATMs*," atm marketplace, Feb 8, 2013.
[31] Adam Vrankuli, "Facial recognition service profiles customer habits, age, gender," Biometric Update.com, Nov 15, 2012.
[32] Steve McClellan, "Nielsen Explores Facial Recognition Tech for Ratings," MediaPost News, Jan 22, 2013.
[33] Article 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services*, March 22, 2012.
[34] Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, April 27, 2012.
[35] Adi Robertson, "Facebook deletes European facial recognition data, satisfying German privacy agency," the Verge, Feb 7, 2013.
[36] The Federal Trade Commission, *Facing Facts: Best practices for Common Uses of Facial Recognition Technologies*, October 2012.
[37] Rob Hastings, "*New HD CCTV puts human rights at risk*," The Independent, Oct 3, 2012.
[38] Daniel J. Solove, "The Virtues of Anonymity," The New York Times, June 20, 2012.
[39] Ian Kerr and jennifer barrigar, "Privacy, Identity and Anonymity", A chapter adapted from Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, Oxford university Press, 2009.
[40] Neil M. Richards, The Dangers of Surveillance," Harvard Law Review, Volume 126, 2013.
[41] Lucas D. Introna and Helen Nissenbaum, "Facial Recognition Technology: A Survey of Policy and Implementation Issues," The Center for Catastrophe Preparedness and Response, New York University.