FACIAL RECOGNITION DEVICES: DEVELOPMENTS AND ISSUES - AN IPR PERSPECTIVE

Lipsa Dash & Parimita Dash*

Abstract

Technology has shifted the paradigm to digital based life from real life. The world of online transactions, ATM's, finger print based attendance system etc. demand a step ahead for identification of the authorized user giving rise to biometric recognition system. The Physiological biometric system which includes facial recognition system has grown. The last few years have witnessed the developments, use and the issues in relation with the technology due to the databases created to store the images and the personal information of the individual for future recognition. The article shows the working and implementation of the service. The article also shows the values and unfortunate lacuna of the software and different sectoral use for its reliable nature. Surveillance cameras are used at border control, prison visitor system, computer and mobile applications security, ATM's becomes easier as it doesn't require a human assistance. This development demands the development of awareness as well as the existing laws for regulating the use of sensitive personal data's and other sensitive information. A few other technologies have also curbed up like assisting the experts in sketching the faces of suspects with the help of witnesses. The intellectual properties involved in the devices are maximum patents. A facial recognition device has connected bio sensors generating billions as being an IP asset for the companies. Apart from phones these devices are attached to drones and other surveillance cameras assisting in search and checks. It helps the enforcement officials to police the populace. They create a template of target faces and then searched in different databases to connect. Similarly the technology behind this is evolving with providing more accuracy to detect and hence the IP market is constantly in competition.

Introduction

Every human has a unique face and it is the unique identification to the race. The devices which were earlier a fantasy are incorporated in our everyday lives now. Starting from companies to residence people have started using it for personal interests and issues. The development of the technology has increased and the growth in the commercial sector has been witnessed increasingly with all kinds of services. Biometric systems are quickly becoming a standard part of modem life as commercial and governmental entities rapidly embrace a technology that promises enhanced security and improved identification.[1] The use of the device should be done in a responsible manner which helps is protect and respect customers privacy and ensure own security too. This device every now and then has helped the society in catching hold of the culprits starting from bank robbery to shop lifting. Earlier the shoplifters after being identified were caught by the security, pictures were clicked and database was updated to list them in the list of probable rouges, but these days a system that scans the face of everyone entering the stores, and suspected shoplifters and alert the store security on their mobile phones.[2] Few companies also use facial recognition software programs to keep their photos organized and secure their devices instead of passwords.[3] Most of the investigation agencies have their way of keeping a record of the faces and the related information that shows their associations with people. The past few years have seen the reliance of people on the technology.[4] A technology has been one of the utilities and backs the nation for its security. Facial recognition is the automatic processing of digital images which contain the faces of individuals for the purpose of identification, authentication/verification or categorization of those individuals. "Facial recognition is variably used starting from photo tagging to social networking sites to security authentication. These technologies have evolved and raise few major privacy concerns as it

* Faculty Associate, KIIT School of Law, KIIT University & Assistant Professor-II, KIIT School of Law, KIIT University, Email Id: lipsadash1993@gmail.com.

[1] Langenderfer J, & Linhoff S, *The Emergence of Biometrics and Its Effect on Consumers,* THE JOURNAL OF CONSUMER AFFAIRS, 39(2), 314-338 (2005).

[2] Jeff John Roberts, *Walmart's Use of Sci-fi Tech to Spot Shoplifters Raises Privacy Questions,* FORTUNE, *(*Nov. 24th, 2019), http://fortune.com/2015/11/09/wal-mart-facial-recognition.

[3] *Future of Privacy Forum*; Working Paper; (Nov. 24th ,2019) https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

[4]Tana Ganeva, *What You Should Know About Face Recognition Technology Used by Police and Spy Agencies Like the NSA*, ALTERNET (Oct. 17, 2019) http://www.alternet.org/what-you-should-know-about-face-recognition-technology-used-police-and-spy-agencies-nsa.

stores the sensitive personal information about people." [5] Facial recognition systems take a facial image; the algorithms measure nodal points creating a numerical code representing the face in the database.[6] The face of every human has approximately 80 nodal points on the face such as the distance between the eyes, the length and width of the nose, the angle of the jaw, depth of the eye socket or the shape of the cheekbones which helps identify the person using the technology.[7] The facial recognition devices carry series of algorithms which analyze the input and distinguish particular facial characteristics using different approaches like the Geometric approach, Photometric approach, Biometric approach and other ways where it calculates the facial features and matches it using a map to get identifiable information. These approaches help the private as well as public sector for arrest, as an evidence, identify and track visitors, track the citizenship of students and persons who seek to study, live or work in the specific country, and to depot undocumented immigrants, and secure the facilities available.[8] The increase of dependency due to its accuracy in the facial recognition technology has developed in years. This technology has integrated into online and mobile services for identification, authentication, verification or categorization of individuals.[9] Even Social networks and other mobile devices use this system.

Developments

According to a survey the facial recognition systems have higher accuracy and faster in terms of technology. It can trace correctly up to 92% of individual data from the database of criminals. The software uses complex mathematical formulas to match the faces with the criminal database.[10] Giant companies like Facebook, Google and Apple have offered automatic facial recognition or detection as a part of their services. For example Facebook prompts to tag the picture as soon as we upload the picture. The rest privacy is controlled in the privacy setting which asks him approval of the person before allowing it in the timeline. The same goes with the Google+ photos which when updated in the Picasa photo editing software links to the user's profile and make clusters of the picture to tag the names instead of going into each picture individually. "The Google+ tags although request for permission to link it to the profile of the

[5] Dr. Joseph Lorenzo Hall, *Facial recognition & Privacy: An EU-US Perspective,* CENTER FOR DEMOCRACY & TECHNOLOGY (Oct 20, 2019), https://www.cdt.org/files/pdfs/CDT_facial_recog.pdf.

[6] Gurpreet Kaur, Manbir Sandhu & Purnima, *Facial Recognition: Issues, Techniques and Applications;* I.J.A.R.C.S.E, (Oct. 23, 2018) http://ijarcsse.com/docs/papers/Volume_6/2_February2016/V6I2-0267.pdf.

[7] *Id.*

[8] Electronic Frontier Foundation (Nov. 24th, 2019), https://www.eff.org/sls/tech/biometrics/faq.

[9] *Supra* note at 5.

[10] Taslitz, A, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions. Law and Contemporary Problems*, 65(2), 125-187.JSTOR (Nov. 24th, 2019), http://www.jstor.org/stable/1192242 doi:1.

user. Facebook reportedly possessed an estimated 60 billion photos by late 2010 (up from 15 billion as of April 2009), with tens of thousands of photos in an average individual."[11] Companies like Facebook, Flickr other online image hosting services use 3rd party software programs like Polar Rose, Riya, Photo Tagger, and Face.com., for identifying faces. Apple bought Rose in 2010 and purchased face.com in 2012 whereas and Google brought Riya.[12] Patenting mobile applications allows developers to prevent others from developing, using or selling the mobile applications without the consent of the developers. [13]

Patent application for example for the celebrity facial recognition was published whose target was for launching of Face Recognition apparel for mobile devices. The application titled *automatically Mining Person Models of Celebrities for Visual Search Applications.* The technology works using an intra model analyzing different combination technologies and precisely identifies amongst the database of the celebrities. The removal of non-face images is an add on. The Chinese State Intellectual property office also applied for a facial recognition technology automatically recognizes multiple known faces in photos or videos on a desktop or mobile device.[14] One of the features enables clustering the face together for easy tagging. The first product of this applied device was Fotobounce which was successful on its performance when tested on Picasa, Microsoft's photo gallery and Apple i-photo. The device was efficient, accurate and the application had speedy stroke. [15] This device helps the companies to ensure the entry of only authorized employees and helps channelizing the person who has access to the confidential information's and holding he/she liable whenever there is a leakage of information. A similar protection and attraction lies with the biometric recognition devices. On 2011, Google created a Face recognizing app which would show the contact details of the person in the picture which was considered very unhealthy and illegal. Every technology has its merits and demerits. Google was also granted patent on device based on facial recognition on a computer. The facial recognition devices at different traffic pints, vehicle accessing premises, linking license plate with owner, authorized drivers etc. can help identify the drivers in using the surveillance cameras to check through its carriage. The potential of the biometrics ace recognition technology has

[11] *supra* note at 6.

[12] *supra* note at 6.

[13] Legasis Newsletter, LEGIST (Nov. 19th, 2019) http://legasis.in/Legist/April2014/html/ipr_mobileapplication.html.

[14] Justin Lee, *Applied Recognition receives two face recognition patents;* BIOMETRIC UPDATE, (Oct. 18th, 2019) http://www.biometricupdate.com/201508/applied-recognition-receives-two-face-recognition-patents

[15] *Id.*

received significant attention in past several years. [16] The facial recognition device has a unique feature of being able to capture the face from a distant location without any actual physical contact. The identification doesn't require a real time interaction and doesn't leave a ambit of ambiguity in recognizing the face when it comes to deterrent purposes. Fundamental shifts in technology and in the economic landscape are rapidly making the current system of intellectual property rights unworkable and ineffective.[17] Sectors starting from banking, finance, travel and online gaming industries ensure the physical presence of the person. Service of online and offline transactions like the ATM's use Facial recognition devices to reduce fraud. With the increase in multiple unauthorized accounts being opened worldwide, multi factor authentication system is a must. [18] At a point where all the forensic evidences leave off the facial recognition technology comes into play by identifying a person based on a photograph or video still. Technologies such as Google Glass, closed circuit television (CCTV) systems, camera phones, other wearable devices make data collection easier.[19]

The conventional way of visitor system during entry and exits are now replaced with Face Recognition Solutions.[20] In India, ensuring beneficiaries for health services in remote places (rural and semi rural areas) use facial recognition devices to make sure the reach of services in the right time and right place through the on-field employees. A number of new techniques like the Smart Attendance, mobile based face recognition and tracking solution now collects bio metric data along with GPS and a time stamp to detect and identify different people at meeting venues and know their exact presence in the venues enabling the organization to track, monitor and audit the data coming from service locations across the country. The visual dashboards have eased the Salary calculations, productivity analysis and auditing.[21] Even Church's around covers the premises with CCTV cameras for surveillance and check the attendance of the members especially during events. Different ATM's in India use high resolution cameras with a notice that his/her photograph will be taken for security purpose. It stores the data in its database. At

[16] *Overview of Facial Recognition Solution*, NEC TECHNOLOGIES INDIA PVT LTD, (Nov. 18th ,2019) http://in.nec.com/en_IN/products/public-safety-security/technology/overview-facial-recognition-solution.html

[17] Lester C.Thurow, *Needed: A New system of Intellectual Property Rights*; HARV.BUS.REV (Nov. 20th ,2019) https://hbr.org/1997/09/needed-a-new-system-of-intellectual-property-rights

[18] Ian Barker, *Adding facial recognition to mobile helps reduce fraud*, BETA NEWS, (Nov. 23rd ,2019) http://betanews.com/2016/10/24/mobile-facial-recognition.

[19] *Id.*

[20] *Supra* note at 7.

[21] *World's Top 10 Usage of Face Recognition Technology*; AINDRA (Oct. 24th 2019) https://aindrasystems.wordpress.com/2015/08/26/worlds-top-10-usage-of-face-recognition-technology-2015.

various voting booths the database of all voters is created, it can be recommended that a facial recognition system should be equipped at booths to prevent any kind of disturbance. The photograph will permit access after matching with the database. India looks forward to Passport and visa verification using the technology.[22] Further developing facial recognition devices to grant driving license can be used. It can be suggested to install these technologies at different public places. These technologies are already installed at different defense and security stops. Verification and Identification of different criminals at any place with an alert service can be expected in the coming few years. The vaults and lockers in banks can be modified with facial recognition devices and authorization would depend on alternative biometric services. Surveillance cameras are used at border control, prison visitor system, computer and mobile applications security, ATM's becomes easier as it doesn't require a human assistance.

Issues

The issues which can be identified on such effective devices are like not being able to trace the face when there is a poor lighting condition, masks covered, sunglasses etc. lowering the resolution and accuracy of image capturing. The effectiveness gets a little compromised if the resolution of camera is not much good which decreases the image quality, size, face angles, lacuna in case of identifying identical twins as finger prints and iris scanning gets more authentic. Few cases were reported where the inability of capturing dark skinned people was highlighted. As per a newspaper report the mismatch of facial recognition led to the detention of a man who was already busy at a different place all together. [23] The arrest was done on basis of a recorded clip from the CCTV camera which stated that he robbed. Many persons also see CCTV as an invasion to privacy.[24] Similarly there are few concerns that have been raised and a proposal[25] was made in the Leadership conference at The American Civil Liberties union which suggested for investigations by police with the use of facial recognition technology. Few laws have been evolved like the Patriot Act of 2001, was passed that enhances the powers of government bodies and the police with respect to the gathering of information, arrest and

[22] *Id.*

[23] Ava Koffman, Losing Face; *How a facial recognition mis-match can ruin your life*, THE INTERCEPT (Oct. 24th 2019), https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life.

[24] Taslitz, A, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions. Law and Contemporary Problems*, 65(2), 125-187, JSTOR (Oct. 24th 2019), http://www.jstor.org/stable/1192242

[25]Vanita Gupta, *Coalition Letter To The Department Of Justice Civil Rights Division Calling For An Investigation of The Disparate Impact Of Face Recognition On Communities Of Color,* A.C.L.U (Nov 5th 2019), https://www.aclu.org/letter/coalition-letter-department-justice-civil-rights-division-calling-investigation-disparate.

imprisonment, while bypassing the courts.[26] These databases sometimes lead to concerns like wrongful matches leading to wrongful detention, non-reliability of the technology where the data might get compromised which may lead to identity theft, impersonation etc, it doesn't have to always do with criminal justice system,[27] sometime the data is collected by the authorities or heads when they are managing big companies and decide to store the details of their employees to combat any loss of data or identify the person who tries to get access or destroy important information which he/she is unauthorized. Any leakage of data of such kind might bring a loss to the reputation and privacy of the person.

Many theorists and signatories also do not favour the accelerated use of the technology as they feel it threatens the privacy and rights of millions.[28] The letter explains "Face Recognition systems are powerful but they can also be biased". Within every human society, one of those common concepts that are to be understood is Privacy. Due to variable nature of privacy, it's really difficult to reach at a final definition. According to socio-historical context, the connotations of privacy and the social bonds surrounding it differ dramatically.[29] Privacy has been progressively invoked in cases that involve the protection of reputation, information and civil liberties.[30] The surveillance tool of Facebook, twitter and Instagram helped to arrest protestors creating a map to the authorities at California.[31] An article from the independent student newspaper at the Boston University also stated how the police use facial recognition devices and if at all it's a threat to the innocent as they profiling of the database also include the pictures that are never involved in a crime but can very well be targeted.[32] The evolvement of smart security cameras will be able to capture the persons who are texting while driving which can be appreciated as a development which helps the law enforcement officials to spot them. The facial recognition systems are perfectly designed to capture the pictures and keep a record of all

[26] Debbie V. S. Kasper, *The Evolution (Or Devolution) of Privacy,* SOCIOLOGICAL FORUM, 20(1), 69-92; JSTOR (Oct. 24th 2019) http://www.jstor.org/stable/4540882.

[27] *supra* note 12.

[28] Ava Koffman, *Losing Face, How a facial recognition mis-match can ruin your life*; THE INTERCEPT (Oct. 24th 2019) https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/.

[29] Debbie V. S. Kasper, *The Evolution (Or Devolution) of Privacy. Sociological Forum,* 20(1), 69-92. (Oct. 24th 2019) http://www.jstor.org/stable/4540882 (2005).

[30] *Id.*

[31] Rusell Brandom, *Facebook, Twitter & Instagram surveillance tool was used to arrest Baltimore protestors,* THE VERGE, (Oct. 24th, 2019), http://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api.

[32] Kaitlyn Olivier, *Is current police use of facial recognition a threat to the innocent?,* THE DAILY FREE PRESS (Oct. 24th, 2019), http://dailyfreepress.com/2016/10/23/olivier-current-police-use-of-facial-recognition-a-threat-to-the-innocent.

the activities I different multiplexes, airports and other public places without actual knowledge of the passersby. The unique way of mass identification is not possible by other biometrics like fingerprints, iris scans, and other speech recognition devices etc. There has been a recent law the Biometric Information Privacy Act in the U.S which has been a hindrance to Facebook and Google's face scanning acts for popular products like Facebook Moments and Google Photos.

This law has given rise to a spate of lawsuits that allege companies failed to obtain consumers' consent before scanning and storing images of their face.[33] The Indian Ministry of Communication and Information Technology framed a new rule under the Information Technology Act, 2000 namely Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. India has come up with its privacy laws and is also implemented. Previously India had no law to deal with privacy issues. The new laws have given new dimension to directing companies and other entities to start using "reasonable security practices and procedures" while handling "sensitive personal data or information." It has introduced both civil and criminal provisions for respective actions. "Sensitive personal data information" (SDPI) includes physiological condition as well as biometric information which indirectly deal with facial recognition devices. Section 42-A of the IT Act talks about the acts and Section 72-A deals with the imprisonment and damages applicable. Few other developments are the provision of consent for collection, the details provided to the individual for its purpose of collection, rights provided so as to right to access, correct and withdrawal of information etc. These rules aren't applicable to the government. What draws the attention is its comparison with EU directive which has set high standards plus flexibilities and exceptions for the use of such information.

Conclusion

The authors agree to one of the observations made after the reviewing a few literatures is that a rule which has combined effect of the technological approach can give the consumer a greater measure of control over how to use the technology of facial recognition and detection without unduly limiting and creating a balance between rights and benefits.[34] Sensitive data information should not be shared or linked to the profiles which may lead to troublesome to people. A person who is victim of being traced just by a picture and gets the address to harm becomes easy. Every

[33] Jeff John Roberts, *Facebook and Google Really Want to Kill This Face-Scanning Law,* FORTUNE (Nov. 26th, 2019), http://fortune.com/2016/06/30/facebook-google-facial-recognition-lawsuits.

[34] s*upra* note at 6.

individual has the right to have information about the privacy and to prevent the disclosure of personal information.[35] Time to time update of the person's profiling should be done. There should be laws for governing the use of such technologies, ensuring its accuracy and to curb biasness, i.e., regulates the use in both public and private sector. There should be true preservation of privacy. The governing principles should take care of taking the consent of the people and individuals should have a choice to how their information is used and distributed.[36] It is concluded that the right of the individual to be free from unwanted and unwarranted governmental intrusion in matters affecting fundamental rights should not narrow or restrict their utility. India has few technologies which were listed in the World Top 10 Usage with respect to face recognition.[37]

[35] Debbie V. S. Kasper, *The Evolution (Or Devolution) of Privacy. Sociological Forum*, 20(1), 69-92 (Oct. 24th 2019) http://www.jstor.org/stable/4540882.

[36] Langenderfer J & Linhoff S, *The Emergence of Biometrics and Its Effect on Consumers*. The Journal of Consumer Affairs, 39(2), 314-338 (2005).

[37] *World's Top 10 Usage of Face Recognition Technology*, AINDRA (Oct. 24th 2019) https://aindrasystems.wordpress.com/2015/08/26/worlds-top-10-usage-of-face-recognition-technology-2015.