Ethics of Facial Recognition Technology

David Avexander, Jacob Richert-Boe

Introduction
In July of 2001, construction worker Rob Milliron was eating lunch in Tampa, Florida’s Ybor City entertainment district. Unbeknownst to Mr. Milliron, a hidden government surveillance camera was using facial recognition technology in an attempt to identify criminals. As Mr. Milliron ate his lunch, these facial recognition systems captured and stored his image. Without Mr. Milliron’s consent, his photograph was taken and used in a U.S. News & World Report article regarding facial recognition technology. The accompanying headline read: "You can’t hide those lying eyes in Tampa."

A woman in Oklahoma saw the picture, misidentified Milliron as her ex-husband wanted on child neglect charges, and called the police. After convincing police he had never been married, had kids, or even been to Oklahoma, he told the St. Petersburg Times, "They made me feel like a criminal."(Kopel & Krause, 2002). Cases like Mr. Milliron’s showcase the issues surrounding the use of facial recognition technology in public places and the need to address them.

Facial Recognition Technology’s Recent History
Since its introduction to the American public in 2001, facial recognition technology has grown rapidly and interest in these systems is increasing. Facial recognition systems are computer-based security systems that are capable of identifying specified individuals with the use of surveillance cameras. Complex algorithms are used by these systems to compare the faces observed by these camera systems with a database of individual photographs. This allows individuals to monitor other individuals who come into the camera’s recording range.

The facial recognition process starts by collecting an image from specified security cameras. The system then measures the nodal points on the face such as the distance between the eyes, the shape of the cheekbones, and other distinguishable
features. These nodal points are then compared to the nodal points computed from a database of pictures in order to find a match (EPIC, 2006). This technology is currently being employed by many different businesses and branches of the government in an attempt to improve security. The Department of Homeland Security has spent millions of dollars on cameras with facial recognition capabilities in an attempt to identify potential threats to the American people.

Limitations

Although this technology is being used by many different organizations, a number of issues surround its installation and use. Current facial recognition technology is very inaccurate and has shown to have little or no effect in areas where it was implemented. Inaccuracies have led to a number of false identifications that have been found to harm individuals. These inaccuracies can be attributed to many factors including image quality, variations in light and appearance of individuals, and the size of the photograph database.

Quality of Database Images

One of the main factors limiting the success of these systems is the quality of the images used in the comparisons. In some cases, the images are dated or of low quality. This makes the process of matching photographs difficult for the system. Clear images on both sides of the equation are needed to generate an accurate match. In most cases, however, this is very hard to accomplish and does not occur. Some photographs can be up to five to ten years old; this is concerning because an individual’s facial features are not constant and can change significantly in a short period of time: people age, may grow facial hair, fluctuate in weight, and obtain facial injuries that can all play a part in the success rate of these systems.

The limitations of dated photographs are even more evident when the study conducted by the National Institute of Standards and Technology (NIST) is considered. NIST found a 43% false rejection rate for pictures of the same person taken one and a half years apart (Phillips, Martin, Wilson, & Pryzbocki, 2000). It is unfeasible to continuously collect high resolution up to date photos of the individuals the system is
attempting to monitor. Obtaining photographs of the desired individuals that the system can use for accurate comparisons can be impossible. This also assumes that the systems have photographs of all the people they are trying to monitor and that they know who they are monitoring. These systems are unable to identify everyone who is a potential threat. This technology is useless when it does not have all the photographs required. If these systems don’t have a photograph of certain individuals then their use is of no concern to those individuals.

**Quality of Captured Images**

Image quality is also affected by variations within the photographs captured by the system. Even if these systems were able to collect high quality images of everyone, they still present inaccuracies. In a test conducted by Richard Smith, former head of the Privacy Foundation at Denver University, changes in lighting, eyeglasses, background objects, camera position, facial position, and expression were all found to seriously affected image quality and system accuracy (Kopel & Krause, 2002). In another test conducted by Palm Beach International Airport, the motion of test subject’s heads often had a significant effect on the systems ability to accurately identify target individuals. There was substantial reduction in successful matches if test subjects posed 15 to 30 degrees off of the input camera focal point; eyeglasses were also problematic (Palm Beach, 2002). In effect, a pair of sunglasses and a tilt of the head can be the only thing needed to evade these systems. Even a simple change in facial expression can cause the system to have trouble identifying a match.

**Database Size**

Although image quality does affect the accuracies of facial recognition systems, it is not the only factor leading to these systems inaccuracies. If it was assumed that these systems were capable of acquiring the required quality photographs from both sides of the comparison, they will still make false matches. As the number of photographs stored in the system’s database increases, performance has been shown to steadily decrease. In a vendor test conducted by NIST, the size of the databases affected the accuracy of matches even in the top-ranked system. The best system tested returned an 85%
identification rate on a database of 800 people, 83% on a database of 1600 people, and 73% on a database of just over 37,000 photographs (NIST, 2006). Performance decreased approximately 2-3 percent every time the number of photographs in the database doubled. This presents a huge problem for proposed facial recognition systems because they will be using databases much larger than the ones used in the example. In some systems, more than one image is required to formulate a match. The sizes of these databases are increasing dramatically and with this performance and accuracy will suffer.

**Ineffectiveness in Public Places**

The inaccuracies of current facial recognition systems are clear and because of this their performance has suffered. These systems have shown to have little or no effect in areas where they were implemented. One such case of the systems ineffectiveness occurred in Tampa, Florida. Cameras employed with facial recognition technologies were installed in various high volume areas, including the 2001 Super Bowl, to help identify criminals. They targeted people in these areas and compared their ‘face prints’ to the database of photographs (Kopel & Krause, 2002).

What was intended to help prevent crime and identify criminals turned out to be a complete and utter failure. The system made obvious errors, including matching male and female subjects and subjects with significant differences in age or weight (ACLU, 2002). The program was later abandoned and no positive matches were ever recorded. These systems are incapable of correctly identifying features that would be obvious to humans such as sex or weight. Because of inaccuracies like these, facial recognition systems cannot be trusted to accurately identify anyone. If they have shown to have no effect in public areas and the intent of the systems is to identify criminals, there is no reason for the continued installation and use of these systems because they are not doing their job.

**False Identifications**

Not only are these systems ineffective, they are making false identifications. At Palm Beach International Airport, the capabilities of facial recognition technology were
once again tested. The month-long test compared fifteen employees against a database containing the mug shots of two hundred and fifty airport workers. Nine hundred and fifty eight attempts were made to match the fifteen test employee’s faces to the database. Under optimal conditions, the system succeeded only four hundred and fifty five times. It also returned one thousand and eighty one false alarms (Palm Beach, 2002). The system was unable to detect 52.5% of the people in the database who were scanned. This is hardly a reliable percentage. The high number of false alarms also is of concern. With higher traffic and many more faces to be scanned, the number of people stopped for no reason could be very significant. These inaccuracies can lead these systems to do more harm than good.

**Ethical Issues Surrounding Facial Recognition Technology**

Given the present performance levels and shortcomings, it would be easy to argue that the issue is a nonstarter. The effectiveness of facial recognition is currently questionable, if not laughable. However, the more relevant point is the future of facial recognition systems. With continued research and development, in concert with the inevitable progress in processing power, camera resolution, networks, databases, and improved algorithms, the question is not a matter of if facial recognition will become accurate and effective, but when will it become accurate and effective. Thus, the question is not one of technology but one of ethics. Even when the technology’s existing deficiencies are addressed, there still remains the question of the ethics of facial recognition technology. The use of facial recognition in public places is unethical, primarily due to privacy concerns, but the ethics of the company/media portrayals of said systems also need to be examined.

Many believe that ethical dilemmas can be resolved by merely consulting codified ethics for a given organization or field. There are relevant codes of ethics for those employed in computer related fields which address the development, engineering, and application of programs and systems as they pertain specifically to privacy. The ACM (Association for Computing Machinery) code of ethics lists the following points:

1.1 Contribute to society and human well-being.
When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways…

1.7 Respect the privacy of others.
Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

Members of the AITP (Association of Information Technology Professionals) pledge the following:

In recognition of my obligation to society I shall:

- Protect the privacy and confidentiality of all information entrusted to me.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.

Finally the Software Engineering code of ethics includes the following:
Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

1.3 Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.

These are salient points and would seem to have a direct bearing on the development and deployment of facial recognition systems. Each of these codes specifically addresses privacy as a primary concern that should be preserved in all aspects of developing and deploying technology. Unfortunately these codes of ethics do not
provide an ethical framework which can be used to discern the ethics of facial recognition systems. Instead, the codes of ethics simply reduce to value judgments as those involved in the development and deployment of these systems may believe they are being used in socially responsible ways and that sufficient steps have been taken to protect the privacy of those subjected to the systems (Bowyer, 2003).

The ethics of the claims regarding the performance and effectiveness of facial recognition systems by the media, and those companies selling the systems, merits some consideration. In a Time article about the use of facial recognition at Super Bowl XXXV the author, Lev Grossman, states, “The beauty of the system is that it is disguise-proof. You can grow a beard and put on sunglasses, and FaceTrac will still pick you out of a crowd” (Time 2001). While the claim sounds reassuring, in reality it is certainly not accurate as studies have shown.

In a study conducted by NIST, changes in illumination, facial position, temporal (time between image captures), distance from the camera, facial expression, and the cameras used to capture images, were all found to adversely affect performance of these systems, sometimes to the point of being completely ineffective (NIST 2000). Tom Colatosti, chief executive of Viisage Technology Inc., made this claim after the September 11th, 2001 terrorist attacks: “If our technology had been deployed, the likelihood is [the terrorists] would have been recognized.” This claim is highly unlikely as only two of the 19 hijackers were known to the FBI and CIA and there is no photo database of terrorists (9-11 Commission 2005). Ethically questionable performance claims only serve to undermine industry credibility and trust. It is in the long-term self-interest of the purveyors of these systems to not misrepresent or mislead in regards to the performance and capabilities of facial recognition systems.

Next there is the question of government invasion of privacy through the use of facial recognition technology. Current legal doctrine, as decided by the Supreme Court, holds that there is little or no expectation of privacy in public and thus there is no infringement of privacy by use of facial recognition in public places. This view does not account for the advancement of technology and the implications it portends for privacy. Just as technological advances required re-interpretation of legal doctrine concerning eavesdropping, which led to the Supreme Court’s decision of a reasonable expectation of
privacy in Katz v. United States in 1967, so too there is hope that current legal interpretation will be updated in response to the threats posed by facial recognition systems. However, even given the fact that the use of these systems may be legal currently, it does not follow that said use is ethical.

Although there is significant philosophical debate about the exact source, nature, and extent of privacy, the threat posed by facial recognition technology is potentially so dire, to any and all forms of privacy, that facial recognition systems should, ideally, be prohibited. A person could be captured by the system anywhere and at anytime. This might reveal those with whom they associate and causes they support, without their consent. What if someone’s face is captured in the “wrong” part of town, or with the “wrong” people? What of the face captured at the abortion clinic or gay-rights meeting, leading to that individual being labeled and categorized in a potentially unfavorable manner? The aspect that makes this all the more egregious is the current ineffectiveness of the systems and the potential for false identification as happened to Rob Milliron.

These systems are taking a photograph of each individual who passes by them. It is unknown how long these photographs will be stored and who will have access to them. This creates the opportunity for misuse of this information. Mr. Milliron had no way to consent to his photograph being taken and used in a national periodical. It is not known how these images will be used or distributed. Even if the person being monitored has not committed an illegal or questionable act, these systems can still have negative effects for the people they are photographing. Mr. Milliron was eating lunch and he was apprehended by the police and questioned. The potential for similar kinds of misuse is clearly present and can deter people from doing anything in public places if they know there is a chance they will be monitored and possibly prosecuted for everyday acts.

The threat posed to privacy by facial recognition technology far outweighs any possible benefits of the technology. As Philip E. Agre, of the University of California, Los Angeles argues, “The potential for abuse is astronomical. Pervasive automatic face recognition could be used to track individuals wherever they go. Systems operated by different organizations could easily be networked to cooperate in tracking an individual from place to place, whether they know the person’s identity or not, and they can share whatever identities they do know.” (Agre 2003). This raises the salient point of the
inevitability of these systems being networked, databases being shared, and individuals being tracked in real-time, all to the detriment of personal privacy and dignity. The self-censorship affected by the ubiquitous use of cameras is degrading and an affront to human dignity. In Great Britain it was discovered that “the people behind [the cameras] are zooming in on unconventional behavior in public that has nothing to do with terrorism”. “And rather than thwarting serious crime, the cameras are being used to enforce social conformity…” (Rosen 2001) Should it really be necessary to constantly feel the need to self-censor and relinquish control to the faceless figures behind the cameras for fear of being caught doing something not even remotely illegal, but which might be construed or portrayed in an unflattering way?

**Recommendations For the Future of Facial Recognition Software**

Because of the threat posed by facial recognition technology, policies and laws need to be enacted that will, if not forbid their use, at least provide the necessary protections to curtail the obvious threat these systems pose to personal privacy. Currently there are no laws governing facial recognition technology, but federally mandated policies are clearly needed. Issues that need to be addressed are many and varied but at a minimum include the following:

- Who gets to add pictures to the database of wanted faces?
- What oversight will be implemented for adding pictures to the database to avoid abuse, personal gain, or conflicts of interest?
- How long do pictures stay in the database?
- Who has access to the database, internally and externally?
- What protections are required to secure the database?
- Under what conditions will the database be shared with other agencies or companies?
- What recourse do people have if they are entered into the database incorrectly?

Until these most basic questions are answered, and avenues of recourse made available to correct misidentification, the use of facial recognition technology should be proscribed in the interest of an individual’s right to privacy.
<http://www.aclu.org/privacy/gen/14802prs20020103.html>

ACM. “ACM Code of Ethics and Professional Conduct” ACM.org. 16 October 1992
<http://www.acm.org/constitution/code.html>

<http://polaris.gseis.ucla.edu/pagre/bar-code.html>

AITP. “Code of Ethics” AITP.org. 2006
<http://www.aitp.org/organization/about/ethics/ethics.jsp>


<http://www.reason.com/0210/fe.dk.face.shtml>


NIST. “Facial Recognition Vendor Test 2002: Overview and Summary”. NIST.gov. 10 October 2006
Palm Beach County Department of Airports. (2002). Facial Recognition System Test (Phase I) Summary. Palm Beach, Florida.